

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

01 - 15 May 2023

Vol. 10 No. 09

Table of Content		
Vendor	Product	Page Number
Application		
8web	read_more_without_refresh	1
9seeds	cptspeakers	1
advancedcustomfields	advanced_custom_fields	1
agentevolution	impress_listings	2
agilepoint	agilepoint_nx	3
Amazon	opensearch	4
A muzon	opensearch_security	5
amr-ical-events- list_project	amr-ical-events-list	7
answer	answer	8
antabot_white- jotter_project	antabot_white-jotter	8
	airflow	9
	brpc	10
Apache	couchdb	11
	log4cxx	13
	spark	18
appim	appium-desktop	22
Apple	safari	23
nppic	xcode	24
archerirm	archer	25
artisanworkshop	japanized_for_woocommerce	26
asmbb_project	asmbb	26
Atlassian	confluence_data_center	27
	confluence_server	29
avirato	hotels_online_booking_engine	31
azuracast	azuracast	32

Vendor	Product	Page Number
basixonline	nex-forms	32
beetl_project	beetl	33
billing_management_syst em_project	billing_management_system	33
bing_site_verification_pl ugin_using_meta_tag_pro ject	bing_site_verification_plugin_using_meta_tag	34
blackandwhitedigital	treepress	34
blueglass	jobs_for_wordpress	35
booqable	rental_software_booqable_rental	35
bumsys_project	bumsys	35
byconsole	pickup_\ _delivery_\ _dine-in_date_time	37
catchthemes	darcie	37
catontechnology	caton_prime	38
catontechnology	ctp_relay_server	38
Cesanta	mjs	39
Chamilo	chamilo_lms	39
churchcrm	churchcrm	42
clio	clio_grow	43
cloud_manager_project	cloud_manager	43
cltphp	cltphp	43
cms_press_project	cms_press	44
codestag	stagtools	44
controlid	rhid	45
convertbox	convertbox_auto_embed	45
creativethemes	blocksy_companion	46
crmeb	crmeb	46
custom_login_page_proje ct	custom_login_page	47
custom_more_link_compl ete_project	custom_more_link_complete	47
cybonet	pineapp_mail_secure	47
Dell	alienware_command_center	48
	command_\ _monitor	48

Vendor	Product	Page Number
Dell	elastic_cloud_storage	49
devolutions	devolutions_server	50
digitaldruid	hotel_druid	50
disqus_conditional_load_ project	disqus_conditional_load	50
Djangoproject	django	51
dmtf	libspdm	52
douphp	douphp	54
dreamer_cms_project	dreamer_cms	55
e-office	e-office	55
easytor	easytor	56
easy_event_calendar_pro ject	easy_event_calendar	57
echa.europa	iuclid	57
effectindex	tripreporter	58
ejs	ejs	59
Elastic	filebeat	60
Elastic	kibana	60
emqx	nanomq	61
enable\/disable_auto_lo gin_when_register_proje ct	enable\/disable_auto_login_when_register	62
Enalean	tuleap	62
enhanced_wp_contact_fo rm_project	enhanced_wp_contact_form	63
Esri	portal_for_arcgis	63
evasys	evasys	66
exquisite_paypal_donati on_project	exquisite_paypal_donation	68
eyes_only_user_access_sh ortcode_project	eyes_only_user_access_shortcode	68
	big-ip_access_policy_manager	69
F5	big-ip_advanced_firewall_manager	83
	big-ip_advanced_web_application_firewall	91

Vendor	Product	Page Number
	big-ip_analytics	100
	big-ip_application_acceleration_manager	109
	big-ip_application_security_manager	118
	big-ip_application_visibility_and_reporting	126
	big-ip_carrier-grade_nat	135
	big-ip_ddos_hybrid_defender	144
	big-ip_domain_name_system	153
	big-ip_edge_gateway	164
	big-ip_fraud_protection_service	173
	big-ip_global_traffic_manager	182
F5	big-ip_link_controller	190
	big-ip_local_traffic_manager	199
	big-ip_next_service_proxy_for_kubernetes	208
	big-ip_policy_enforcement_manager	208
	big-ip_ssl_orchestrator	217
	big-ip_webaccelerator	226
	big-ip_websafe	235
	big-iq_centralized_management	243
	nginx_api_connectivity_manager	244
	nginx_instance_manager	245
	nginx_security_monitoring	246
fareharbor	fareharbor	248
fastlinemedia	customizer_export\/import	248
Fedoraproject	extra_packages_for_enterprise_linux	249
finviz	stock_market_charts_from_finviz	250
firecask_like_\&_share_b utton_project	firecask_like_\&_share_button	250
food_ordering_managem ent_system_project	food_ordering_management_system	250
Fortinet	fortiadc	251
	fortinac	253
	fortinac-f	254
	fortiproxy	255

Vendor	Product	Page Number
fullworksplugins	quick_paypal_payments	258
funadmin	funadmin	259
geminilabs	site_reviews	260
genomedics	millegpg	260
Geovision	gv-edge_recording_manager	260
getrebuild	rebuild	261
ghost	ghost	262
gin-gonic	gin	263
Gitlab	gitlab	264
givewp	givewp	281
gmo	typesquare_webfonts_for_conoha	281
Google	chrome	282
doogle	web_stories	285
greentreelabs	circles_gallery	287
hashicorp	vault	287
hu-manity	cookie_notice_\&_compliance_for_gdpr_\/_ccp a	288
	business_automation_workflow	288
	cloudant	295
IBM	elastic_storage_system	297
	mq_appliance	298
	spectrum_scale	299
Illumos	illumos-gate	300
ipandao	editor.md	300
j2eefast	j2eefast	301
jch_optimize_project	jch_optimize	302
jsreport	jsreport	303
judging_management_sy stem_project	judging_management_system	303
kanbanwp	kanban_boards_for_wordpress	304
konga_project	konga	305
lazy_social_comments_pr oject	lazy_social_comments	305

Vendor	Product	Page Number
Libming	libming	305
lightspeedhq	ecwid_ecommerce_shopping_cart	306
limit_login_attempts_pro ject	limit_login_attempts	306
Linuxfoundation	fluid	307
	rekor	309
Llvm	llvm	310
machothemes	newsmag	312
mailbutler	shimo	312
mattermost	mattermost_desktop	313
metaphorcreations	ditty	313
metersphere	metersphere	313
microbin	microbin	314
	365_apps	315
	edge_chromium	315
	office	315
Microsoft	remote_desktop	316
	sharepoint_enterprise_server	316
	sharepoint_server	317
	word	317
monicahq	monica	317
Moodle	moodle	319
multi_language_hotel_ma nagement_software_proj ect	multi_language_hotel_management_software	312
mutagan	mutagen	322
mutagen	mutagen_compose	325
netentsec	application_security_gateway	327
newbee-mall_project	newbee-mall	328
newbinggogo_project	newbinggogo	328
obsidian	obsidian	328
octopus	octopus_deploy	329
olevmedia	olevmedia_shortcodes	329

Vendor	Product	Page Number
online_dj_management_s ystem_project	online_dj_management_system	330
online_food_ordering_sy stem_project	online_food_ordering_system	331
online_pizza_ordering_sy stem_project	online_pizza_ordering_system	331
online_reviewer_system_ project	online_reviewer_system	331
online_tours_\&_travels_ management_system_pr oject	online_tours_\&_travels_management_system	332
onosproject	onos	333
Open-emr	openemr	333
openproject	openproject	334
opentsdb	opentsdb	335
oxilab	accordions	336
palletsprojects	flask	337
peepso	peepso	340
perfreeblog_project	perfreeblog	341
Phpmyfaq	phpmyfaq	341
Pimcore	pimcore	342
pixelyoursite	product_catalog_feed	343
plainviewplugins	mycryptocheckout	344
plugin-planet	dashboard_widget_suite	344
podofo_project	podofo	345
Podsfoundation	pods	346
premmerce	premmerce_redirect_manager	346
Prestashop	prestashop	346
1103(23110)	scexportcustomers	347
profilepress	profilepress	347
properfraction	profilepress	347
publish_to_schedule_proj ect	publish_to_schedule	348
Puppet	puppet_enterprise	348

Vendor	Product	Page Number
Puppet	puppet_server	349
qbian61_forum- java_project	qbian61_forum-java	349
quantumcloud	ai_chatbot	350
rediker	adminplus	352
return_and_warranty_ma nagement_system_for_w oocommerce_project	return_and_warranty_management_system_fo r_woocommerce	352
rosariosis	rosariosis	353
S-cms	S-cms	353
Samsung	samsung_blockchain_keystore	353
Samsung	samsung_core_services	355
sandhillsdev	easy_digital_downloads	356
	businessobjects	356
	businessobjects_business_intelligence	358
	business_planning_and_consolidation	363
	customer_relationship_management_s4fnd	364
	customer_relationship_management_webclien t_ui	370
	gui_for_windows	383
SAP	netweaver_application_server_for_java	384
	powerdesigner_proxy	385
	s4core	386
	s4fnd	386
	sapscore	392
	sapui5	393
	vendor_master_hierarchy	397
scanservjs_project	scanservjs	404
Sem-cms	Semcms	405
seopress	seopress	405
simple_portfolio_gallery_ project	simple_portfolio_gallery	405
simple_youtube_respons ive_project	simple_youtube_responsive	406

Vendor	Product	Page Number
sloth_logo_customizer_pr oject	sloth_logo_customizer	406
smtp_mailing_queue_pro ject	smtp_mailing_queue	407
socket	engine.io	407
sponsors_carousel_proje ct	sponsors_carousel	408
sticky_ad_bar_project	sticky_ad_bar	408
strikingly	strikingly	409
struktur	libheif	410
supportcandy	supportcandy	410
surbma	gdpr_proof_cookie_consent_\&_notice_bar	410
Suse	rancher	411
tapfiliate	tapfiliate	412
te-st	yandex.news_feed_by_teplitsa	412
Teampass	teampass	412
themeisle	visualizer	413
timersys	wp_popups	414
Tipsandtricks-hq	category_specific_rss_feed_subscription	414
tms-outsource	wpdatatables	414
	mega_addons_for_wpbakery_page_builder	415
topdigitaltrends	ultimate_carousel_for_elementor	415
	ultimate_carousel_for_wpbakery_page_builder	416
tortall	yasm	416
total-soft	video_gallery	417
totaljs	flow	418
	messenger	418
tribe29	checkmk	419
triton_project	triton	420
typecho	typecho	423
usbmemorydirect	simple_custom_author_profiles	423
userlike	userlike	423

Vendor	Product	Page Number
vertical_scroll_recent_po st_project	vertical_scroll_recent_post	424
VIM	vim	424
virtualreception	digital_reciptie	425
vk.company	mymail	425
vslider_multi_image_slid er_project	vslider_multi_image_slider	425
W3	webassembly	426
web_design_easy_sign_up _project	web_design_easy_sign_up	426
winterchen	my-site	426
winwar	wp_email_capture	427
wjjsoft	innokb	427
	download_manager	428
wpdownloadmanager	gutenberg_blocks_for_wordpress_download_m anager	428
wpinventory	wp_inventory_manager	429
wpmart	team_memberteam_with_slider	429
wpmobile.app_project	wpmobile.app	429
wpruby	ruby_help_desk	430
wp_baidu_submit_projec t	wp_baidu_submit	430
wp_content_filter _censor_all_offensive_con tent_from_your_site_proj ect	wp_content_filter _censor_all_offensive_content_from_your_site	430
wp_custom_author_url_p roject	wp_custom_author_url	431
wp_login_box_project	wp_login_box	431
wp_open_social_project	wp_open_social	432
wp_resource_download_ management_project	wp_resource_download_management	432
wp_simple_events_projec t	wp_simple_events	432
Zammad	Zammad	433

Vendor	Product	Page Number
zhenfeng13_my- blog_project	zhenfeng13_my-blog	433
Zohocorp	manageengine_opmanager	434
zyrex	рорир	435
Hardware		
	eki-1521	435
Advantech	eki-1522	437
	eki-1524	438
aigital	wireless-n_repeater_mini_router	440
Amazon	fire_tv_stick_3rd_gen	440
Apple	studio_display	442
Asus	rt-ac51u	442
bestbuy	insignia_tv	443
Cisco	spa112	444
	dir-8681	445
Dlink	dir-879	446
	dir-8901	446
ez-net	next-7004n	446
feiyuxing	vec40g	447
fiio	m6	448
	wallbox_glb	448
garo	wallbox_gtb	448
	wallbox_gtc	449
gl-inet	gl-mt3000	449
НЗС	gr-1200w	450
НР	integrated_lights-out	450
111	proliant_rl300	451
IBM	3948-ved	451
	3957-vec	452
	3957-ved	452
	smart_clock_essential_with_alexa_built_in	452
Lenovo	thinkagile_hx1021	453
	thinkagile_hx1320	453

Vendor	Product	Page Number
	thinkagile_hx1321	454
	thinkagile_hx1331	455
	thinkagile_hx1520-r	455
	thinkagile_hx1521-r	456
	thinkagile_hx2320-e	457
	thinkagile_hx2321	457
	thinkagile_hx2330	458
	thinkagile_hx2331	458
	thinkagile_hx2720-e	459
	thinkagile_hx3320	460
	thinkagile_hx3321	460
	thinkagile_hx3330	461
	thinkagile_hx3331	462
	thinkagile_hx3375	462
	thinkagile_hx3376	463
Lenovo	thinkagile_hx3520-g	463
Lenovo	thinkagile_hx3521-g	464
	thinkagile_hx3720	465
	thinkagile_hx3721	465
	thinkagile_hx5520	466
	thinkagile_hx5520-c	467
	thinkagile_hx5521	467
	thinkagile_hx5521-c	468
	thinkagile_hx5530	468
thinkagile_hx5531 thinkagile_hx7520 thinkagile_hx7521 thinkagile_hx7530	thinkagile_hx5531	469
	thinkagile_hx7520	470
	thinkagile_hx7521	470
	thinkagile_hx7530	471
	thinkagile_hx7531	472
	thinkagile_hx7820	472
thinkagile_hx7821	473	
	thinkagile_hx_enclosure	473

Vendor	Product	Page Number
	thinkagile_mx1020	474
	thinkagile_mx1021_on_se350	475
	thinkagile_mx3330-f	475
	thinkagile_mx3330-h	476
	thinkagile_mx3331-f	477
	thinkagile_mx3331-h	477
	thinkagile_mx3530-h	478
	thinkagile_mx3530_f	478
	thinkagile_mx3531-f	479
	thinkagile_mx3531_h	480
	thinkagile_vx1320	480
	thinkagile_vx2320	481
	thinkagile_vx2330	482
	thinkagile_vx3320	482
	thinkagile_vx3330	483
Lenovo	thinkagile_vx3331	483
Lenovo	thinkagile_vx3520-g	484
	thinkagile_vx3530-g	485
	thinkagile_vx3720	485
	thinkagile_vx5520	486
	thinkagile_vx5530	487
	thinkagile_vx7320_n	487
	thinkagile_vx7330	488
	thinkagile_vx7520	489
	thinkagile_vx7520_n	489
	thinkagile_vx7530	490
	thinkagile_vx7531	490
	thinkagile_vx7820	491
	thinkagile_vx_1se	492
	thinkagile_vx_2u4n	492
	thinkagile_vx_4u	493
	thinkedge_se450_	493

Vendor	Product	Page Number
	thinkstation_p920	494
	thinksystem_sd530	495
	thinksystem_sd630_v2	495
	thinksystem_sd650	496
	thinksystem_sd650-n_v2	497
	thinksystem_sd650_v2	497
	thinksystem_se350	498
	thinksystem_sn550	499
	thinksystem_sn550_v2	499
	thinksystem_sn850	500
	thinksystem_sr150	500
	thinksystem_sr158	501
	thinksystem_sr250	502
	thinksystem_sr250_v2	502
	thinksystem_sr258	503
Lenovo	thinksystem_sr258_v2	503
Lenovo	thinksystem_sr530	504
	thinksystem_sr550	505
	thinksystem_sr570	505
	thinksystem_sr590	506
	thinksystem_sr630	507
	thinksystem_sr630_v2	507
	thinksystem_sr645	508
	thinksystem_sr645_v3	508
	thinksystem_sr650	509
	thinksystem_sr650_v2	510
	thinksystem_sr665	510
	thinksystem_sr665_v3	511
	thinksystem_sr670	512
	thinksystem_sr670_v2	512
	thinksystem_sr850	513
	thinksystem_sr850p	513

Vendor	Product	Page Number
	thinksystem_sr850_v2	514
	thinksystem_sr860	515
	thinksystem_sr860_v2	515
	thinksystem_sr950	516
	thinksystem_st250	517
Lenovo	thinksystem_st250_v2	517
	thinksystem_st258	518
	thinksystem_st258_v2	518
	thinksystem_st550	519
	thinksystem_st650_v2	520
	thinksystem_st658_v2	520
milesight	ncr\/camera	521
mitrastar	gpt-2741gnac-n2	522
	315_5g_iot_modem	522
	8905	522
	8909	523
	8917	523
	8952	524
	8953	524
	8953pro	524
	8956	525
	8976	525
Qualcomm	8976pro	525
	8998	526
	9206_lte_modem	526
	apq5053-aa	526
	apq8017	527
	apq8052	527
	apq8053-aa	527
	apq8053-ac	528
	apq8053-lite	528
	apq8056	529

Vendor	Product	Page Number
	apq8064au	529
	apq8076	529
	aqt1000	530
	ar8031	530
	ar8035	530
	c-v2x_9150	530
	csra6620	531
	csra6640	531
	csrb31024	531
	flight_rb5_5g_platform	531
	home_hub_100_platform	532
	mdm9250	532
	mdm9628	532
	mdm9650	533
	msm8108	533
Ovelesson	msm8209	534
Qualcomm	msm8608	534
	msm8909w	535
	msm8996au	535
	qam8295p	535
	qca-4020-0-217msp	536
	qca-4020-1-217msp	536
	qca-4024-0-68cmqfn	536
	qca-4024-1-68cmqfn	536
	qca6174	537
	qca6174a	537
	qca6310	538
	qca6320	538
	qca6335	538
	qca6390	539
	qca6391	539
	qca6420	540

Vendor	Product	Page Number
	qca6421	540
	qca6426	541
	qca6430	541
	qca6431	542
	qca6436	542
	qca6564	543
	qca6564a	543
	qca6564au	543
	qca6574	544
	qca6574a	544
	qca6574au	545
	qca6584au	545
	qca6595	546
	qca6595au	546
	qca6696	546
Qualaamm	qca6698aq	547
Qualcomm	qca8081	547
	qca8337	548
	qca9367	548
	qca9377	549
	qca9379	549
	qcm2290	549
	qcm4290	550
	qcm6125	550
	qcm6490	551
	qcn6024	551
	qcn9011	551
	qcn9012	552
	qcn9024	552
	qcn9074	552
	qcs2290	553
	qcs400	553

Vendor	Product	Page Number
	qcs410	554
	qcs4290	554
	qcs605	554
	qcs610	555
	qcs6125	555
	qcs6490	556
	qcs8155	556
	qcs8250	557
	qm215	557
	qrb5165	557
	qrb5165m	558
	qrb5165n	558
	qsm8250	559
	sa4150p	559
	sa4155p	559
Qualcomm	sa6145p	560
Qualcomm	sa6150p	560
	sa6155	561
	sa6155p	561
	sa8145p	562
	sa8150p	563
	sa8155	563
	sa8155p	564
	sa8195p	564
	sa8295p	565
	sa8540p	565
	sa9000p	566
	sd626	566
	sd660	566
	sd670	567
	sd675	567
	sd730	568

Vendor	Product	Page Number
	sd835	568
	sd855	569
	sd865_5g	569
	sd888	569
	sda\/sdm845	570
	sdm429	570
	sdm429w	571
	sdm439	571
	sdm450	572
	sdm660	572
	sdm670	572
	sdm710	573
	sdm845	573
	sdx20m	574
	sdx55	574
Qualcomm	sd_675	575
Qualcomm	sm4125	575
	sm4250-aa	576
	sm4350	576
	sm4350-ac	576
	sm4375	577
	sm6115	577
	sm6125	577
	sm6150	578
	sm6150-ac	578
	sm6225	579
	sm6225-ad	579
	sm6250	580
	sm6250p	580
	sm6350	580
	sm6375	581
	sm7125	581

Vendor	Product	Page Number
	sm7150-aa	582
	sm7150-ab	582
	sm7150-ac	582
	sm7225	583
	sm7250-aa	583
	sm7250-ab	584
	sm7250-ac	584
	sm7250p	584
	sm7315	585
	sm7325	585
	sm7325-ae	585
	sm7325-af	586
	sm7325p	586
	sm7350-ab	586
	sm8150	587
Qualcomm	sm8150-ac	587
Qualcomm	sm8250	587
	sm8250-ab	587
	sm8250-ac	588
	sm8350	588
	sm8350-ac	588
	snapdragon_1200_wearable_platform	589
	snapdragon_208_processor	589
	snapdragon_630_mobile_platform	590
	snapdragon_632_mobile_platform	590
	snapdragon_636_mobile_platform	590
	snapdragon_7c\+_gen_3_compute	590
	snapdragon_820_automotive_platform	591
	snapdragon_auto_4g_modem	591
	snapdragon_auto_5g_modem-rf	592
	<pre>snapdragon_w5\+_gen_1_wearable_platform</pre>	592
	snapdragon_wear_2100_platform	592

Vendor	Product	Page Number
	snapdragon_wear_2500_platform	593
	snapdragon_wear_3100_platform	593
	snapdragon_wear_4100\+_platform	593
	snapdragon_x12_lte_modem	594
	snapdragon_x20_lte_modem	594
	snapdragon_x24_lte_modem	594
	snapdragon_x50_5g_modem-rf_system	595
	snapdragon_x55_5g_modem-rf_system	595
	snapdragon_x5_lte_modem	596
	snapdragon_x65_5g_modem-rf_system	596
	snapdragon_xr1_platform	596
	<pre>snapdragon_xr2\+_gen_1_platform</pre>	597
	snapdragon_xr2_5g_platform	597
	ssm7250-aa	598
	sw5100	598
Qualcomm	sw5100p	598
Qualcomm	sxr1120	598
	sxr2130	599
	wcd9326	599
	wcd9330	600
	wcd9335	600
	wcd9340	601
	wcd9341	601
	wcd9370	601
	wcd9371	602
	wcd9375	602
	wcd9380	603
	wcd9385	603
	wcn3610	604
	wcn3615	604
	wcn3620	605
	wcn3660	605

Vendor	Product	Page Number
	wcn3660b	605
	wcn3680	606
	wcn3680b	606
	wcn3910	607
	wcn3950	607
	wcn3980	608
	wcn3988	608
	wcn3990	609
Qualcomm	wcn3998	609
Qualcomm	wcn3999	609
	wcn6740	610
	wcn6750	610
	wcn685x-1	610
	wcn685x-5	611
	wsa8810	611
	wsa8815	612
	wsa8830	612
	wsa8835	613
Deduvelleutemetien	armorstart_st_281e	613
Rockwellautomation	armorstart_st_284ee	620
	exynos	627
	exynos_1080	628
Samsung	exynos_5123	628
	exynos_5300	629
	exynos_980	629
shapeshift	keepkey	630
	6gk1411-1ac00	631
Siemens	6gk1411-5ac00	635
	scalance_lpe9403	639
Tondo	ac18	641
Tenda	n301	641
totolink	a7100ru	642

Vendor	Product	Page Number
totolink	x5000r	643
7.000	Nbg-418n	643
Zyxel	nbg6604	645
Operating System		
	eki-1521_firmware	646
Advantech	eki-1522_firmware	647
	eki-1524_firmware	648
aigital	wireless-n_repeater_mini_router_firmware	650
Amazon	fire_os	650
	ipados	653
	ipad_os	664
	iphone_os	676
Arriela	macos	699
Apple	mac_os_x	741
	studio_display_firmware	742
	tvos	742
	watchos	750
Arubanetworks	arubaos	759
Asus	rt-ac51u_firmware	762
Axis	axis_os	762
Cisco	spa112_firmware	763
contiki-ng	contiki-ng	764
Debian	debian_linux	765
	dir-868l_firmware	770
Dlink	dir-879_firmware	771
	dir-890l_firmware	771
ez-net	next-7004n_firmware	771
Fedoraproject	fedora	772
feiyuxing	vec40g_firmware	780
fiio	m6_firmware	780
Fortinet	fortios	781
garo	wallbox_glb_firmware	785

Vendor	Product	Page Number
<i>a</i> ano	wallbox_gtb_firmware	785
garo	wallbox_gtc_firmware	785
gl-inet	gl-mt3000_firmware	786
Coogle	android	786
Google	chrome_os	787
НЗС	gr-1200w_firmware	787
	arubaos	788
НР	instantos	793
nr	integrated_lights-out_firmware	837
	proliant_rl300_firmware	838
	3948-ved_firmware	838
IBM	3957-vec_firmware	839
IDM	3957-ved_firmware	839
	i	841
kaiostech	kaios	843
	smart_clock_essential_with_alexa_built_in_firm ware	844
	thinkagile_hx1021_firmware	844
	thinkagile_hx1320_firmware	845
	thinkagile_hx1321_firmware	846
	thinkagile_hx1331_firmware	846
	thinkagile_hx1520-r_firmware	847
	thinkagile_hx1521-r_firmware	847
<b>.</b>	thinkagile_hx2320-e_firmware	848
Lenovo	thinkagile_hx2321_firmware	849
	thinkagile_hx2330_firmware	849
	thinkagile_hx2331_firmware	851
	thinkagile_hx2720-e_firmware	851
	thinkagile_hx3320_firmware	852
	thinkagile_hx3321_firmware	852
	thinkagile_hx3330_firmware	853
	thinkagile_hx3331_firmware	854
	thinkagile_hx3375_firmware	855

Vendor	Product	Page Number
	thinkagile_hx3376_firmware	856
	thinkagile_hx3520-g_firmware	856
	thinkagile_hx3521-g_firmware	857
	thinkagile_hx3720_firmware	857
	thinkagile_hx3721_firmware	858
	thinkagile_hx5520-c_firmware	859
	thinkagile_hx5520_firmware	859
	thinkagile_hx5521-c_firmware	860
	thinkagile_hx5521_firmware	860
	thinkagile_hx5530_firmware	861
	thinkagile_hx5531_firmware	862
	thinkagile_hx7520_firmware	862
	thinkagile_hx7521_firmware	863
	thinkagile_hx7530_firmware	864
	thinkagile_hx7531_firmware	864
Lonovo	thinkagile_hx7820_firmware	865
Lenovo	thinkagile_hx7821_firmware	866
	thinkagile_hx_enclosure_firmware	867
	thinkagile_mx1020_firmware	867
	thinkagile_mx1021_on_se350_firmware	868
	thinkagile_mx3330-f_firmware	868
	thinkagile_mx3330-h_firmware	869
	thinkagile_mx3331-f_firmware	870
	thinkagile_mx3331-h_firmware	870
	thinkagile_mx3530-h_firmware	871
	thinkagile_mx3530_f_firmware	872
	thinkagile_mx3531-f_firmware	872
	thinkagile_mx3531_h_firmware	873
	thinkagile_vx1320_firmware	873
	thinkagile_vx2320_firmware	874
	thinkagile_vx2330_firmware	875
	thinkagile_vx3320_firmware	875

Vendor	Product	Page Number
	thinkagile_vx3330_firmware	876
	thinkagile_vx3331_firmware	877
	thinkagile_vx3520-g_firmware	877
	thinkagile_vx3530-g_firmware	878
	thinkagile_vx3720_firmware	878
	thinkagile_vx5520_firmware	879
	thinkagile_vx5530_firmware	880
	thinkagile_vx7320_n_firmware	880
	thinkagile_vx7330_firmware	881
	thinkagile_vx7520_firmware	882
	thinkagile_vx7520_n_firmware	882
	thinkagile_vx7530_firmware	883
	thinkagile_vx7531_firmware	883
	thinkagile_vx7820_firmware	884
	thinkagile_vx_1se_firmware	885
Lonovo	thinkagile_vx_2u4n_firmware	885
Lenovo	thinkagile_vx_4u_firmware	886
	thinkedge_se450_firmware	887
	thinkstation_p920_firmware	887
	thinksystem_sd530_firmware	888
	thinksystem_sd630_v2_firmware	888
	thinksystem_sd650-n_v2_firmware	889
	thinksystem_sd650_firmware	890
	thinksystem_sd650_v2_firmware	890
	thinksystem_se350_firmware	891
	thinksystem_sn550_firmware	892
	thinksystem_sn550_v2_firmware	892
	thinksystem_sn850_firmware	893
	thinksystem_sr150_firmware	893
	thinksystem_sr158_firmware	894
	thinksystem_sr250_firmware	895
	thinksystem_sr250_v2_firmware	895

Vendor	Product	Page Number
	thinksystem_sr258_firmware	896
	thinksystem_sr258_v2_firmware	897
	thinksystem_sr530_firmware	897
	thinksystem_sr550_firmware	898
	thinksystem_sr570_firmware	898
	thinksystem_sr590_firmware	899
	thinksystem_sr630_firmware	900
	thinksystem_sr630_v2_firmware	900
	thinksystem_sr645_firmware	901
	thinksystem_sr645_v3_firmware	902
	thinksystem_sr650_firmware	902
	thinksystem_sr650_v2_firmware	903
	thinksystem_sr665_firmware	903
	thinksystem_sr665_v3_firmware	904
Lenovo	thinksystem_sr670_firmware	905
	thinksystem_sr670_v2_firmware	905
	thinksystem_sr850p_firmware	906
	thinksystem_sr850_firmware	907
	thinksystem_sr850_v2_firmware	907
	thinksystem_sr860_firmware	908
	thinksystem_sr860_v2_firmware	908
	thinksystem_sr950_firmware	909
	thinksystem_st250_firmware	910
	thinksystem_st250_v2_firmware	910
	thinksystem_st258_firmware	911
	thinksystem_st258_v2_firmware	912
	thinksystem_st550_firmware	912
	thinksystem_st650_v2_firmware	913
	thinksystem_st658_v2_firmware	913
Linux	linux_kernel	914
Microsoft	windows	919
MICI 05011	windows_10_1507	920

Vendor	Product	Page Number
	windows_10_1607	923
	windows_10_1809	926
	windows_10_20h2	929
	windows_10_21h2	932
	windows_10_22h2	936
Microsoft	windows_11_21h2	939
	windows_11_22h2	942
	windows_server_2008	946
	windows_server_2012	951
	windows_server_2016	956
	windows_server_2019	959
	windows_server_2022	962
milesight	ncr\/camera_firmware	965
mitrastar	gpt-2741gnac-n2_firmware	966
	315_5g_iot_modem_firmware	966
	8905_firmware	967
	8909_firmware	967
	8917_firmware	967
	8952_firmware	968
	8953pro_firmware	968
	8953_firmware	969
	8956_firmware	969
Qualcomm	8976pro_firmware	969
Qualcomm	8976_firmware	970
	8998_firmware	970
	9206_lte_modem_firmware	970
	apq5053-aa_firmware	971
	apq8017_firmware	971
	apq8052_firmware	971
	apq8053-aa_firmware	971
	apq8053-ac_firmware	972
	apq8053-lite_firmware	972

Vendor	Product	Page Number
	apq8056_firmware	973
	apq8064au_firmware	973
	apq8076_firmware	973
	aqt1000_firmware	974
	ar8031_firmware	974
	ar8035_firmware	974
	c-v2x_9150_firmware	974
	csra6620_firmware	975
	csra6640_firmware	975
	csrb31024_firmware	975
	flight_rb5_5g_platform_firmware	975
	home_hub_100_platform_firmware	976
	mdm9250_firmware	976
	mdm9628_firmware	976
	mdm9650_firmware	977
Qualcomm	msm8108_firmware	977
Qualcomm	msm8209_firmware	978
	msm8608_firmware	978
	msm8909w_firmware	979
	msm8996au_firmware	979
	qam8295p_firmware	979
	qca-4020-0-217msp_firmware	980
	qca-4020-1-217msp_firmware	980
	qca-4024-0-68cmqfn_firmware	980
	qca-4024-1-68cmqfn_firmware	980
	qca6174a_firmware	981
	qca6174_firmware	981
	qca6310_firmware	982
	qca6320_firmware	982
	qca6335_firmware	982
	qca6390_firmware	983
	qca6391_firmware	983

Vendor	Product	Page Number
	qca6420_firmware	984
	qca6421_firmware	984
	qca6426_firmware	985
	qca6430_firmware	985
	qca6431_firmware	986
	qca6436_firmware	986
	qca6564au_firmware	986
	qca6564a_firmware	987
	qca6564_firmware	987
	qca6574au_firmware	988
	qca6574a_firmware	988
	qca6574_firmware	989
	qca6584au_firmware	989
	qca6595au_firmware	990
	qca6595_firmware	990
Qualcomm	qca6696_firmware	990
Qualcomm	qca6698aq_firmware	991
	qca8081_firmware	991
	qca8337_firmware	992
	qca9367_firmware	992
	qca9377_firmware	993
	qca9379_firmware	993
	qcm2290_firmware	993
	qcm4290_firmware	994
	qcm6125_firmware	994
	qcm6490_firmware	995
	qcn6024_firmware	995
	qcn9011_firmware	995
	qcn9012_firmware	996
	qcn9024_firmware	996
	qcn9074_firmware	996
	qcs2290_firmware	997

Vendor	Product	Page Number
	qcs400_firmware	997
	qcs410_firmware	998
	qcs4290_firmware	998
	qcs605_firmware	998
	qcs610_firmware	999
	qcs6125_firmware	999
	qcs6490_firmware	1000
	qcs8155_firmware	1000
	qcs8250_firmware	1001
	qm215_firmware	1001
	qrb5165m_firmware	1001
	qrb5165n_firmware	1002
	qrb5165_firmware	1002
	qsm8250_firmware	1003
	sa4150p_firmware	1003
Qualcomm	sa4155p_firmware	1003
Qualcomm	sa6145p_firmware	1004
	sa6150p_firmware	1004
	sa6155p_firmware	1005
	sa6155_firmware	1005
	sa8145p_firmware	1006
	sa8150p_firmware	1007
	sa8155p_firmware	1007
	sa8155_firmware	1008
	sa8195p_firmware	1008
	sa8295p_firmware	1009
	sa8540p_firmware	1009
	sa9000p_firmware	1010
	sd626_firmware	1010
	sd660_firmware	1010
	sd670_firmware	1011
	sd675_firmware	1011

Vendor	Product	Page Number
	sd730_firmware	1012
	sd835_firmware	1012
	sd855_firmware	1013
	sd865_5g_firmware	1013
	sd888_firmware	1014
	sda\/sdm845_firmware	1014
	sdm429w_firmware	1014
	sdm429_firmware	1015
	sdm439_firmware	1015
	sdm450_firmware	1016
	sdm660_firmware	1016
	sdm670_firmware	1017
	sdm710_firmware	1017
	sdm845_firmware	1017
	sdx20m_firmware	1018
Qualcomm	sdx55_firmware	1018
Qualcomm	sd_675_firmware	1019
	sm4125_firmware	1019
	sm4250-aa_firmware	1020
	sm4350-ac_firmware	1020
	sm4350_firmware	1020
	sm4375_firmware	1021
	sm6115_firmware	1021
	sm6125_firmware	1021
	sm6150-ac_firmware	1022
	sm6150_firmware	1022
	sm6225-ad_firmware	1023
	sm6225_firmware	1023
	sm6250p_firmware	1024
	sm6250_firmware	1024
	sm6350_firmware	1025
	sm6375_firmware	1025

Vendor	Product	Page Number
	sm7125_firmware	1025
	sm7150-aa_firmware	1026
	sm7150-ab_firmware	1026
	sm7150-ac_firmware	1027
	sm7225_firmware	1027
	sm7250-aa_firmware	1028
	sm7250-ab_firmware	1028
	sm7250-ac_firmware	1028
	sm7250p_firmware	1029
	sm7315_firmware	1029
	sm7325-ae_firmware	1029
	sm7325-af_firmware	1030
	sm7325p_firmware	1030
	sm7325_firmware	1030
	sm7350-ab_firmware	1030
	sm8150-ac_firmware	1031
Qualcomm	sm8150_firmware	1031
	sm8250-ab_firmware	1031
	sm8250-ac_firmware	1032
	sm8250_firmware	1032
	sm8350-ac_firmware	1032
	sm8350_firmware	1033
	snapdragon_1200_wearable_platform_firmwa re	1033
	snapdragon_208_processor_firmware	1033
	snapdragon_630_mobile_platform_firmware	1034
	snapdragon_632_mobile_platform_firmware	1034
	snapdragon_636_mobile_platform_firmware	1034
	snapdragon_7c\+_gen_3_compute_firmware	1035
	snapdragon_820_automotive_platform_firmwa re	1035
	snapdragon_auto_4g_modem_firmware	1035
	snapdragon_auto_5g_modem-rf_firmware	1036

Vendor	Product	Page Number
	snapdragon_w5\+_gen_1_wearable_platform_f irmware	1036
	snapdragon_wear_2100_platform_firmware	1036
	snapdragon_wear_2500_platform_firmware	1037
	snapdragon_wear_3100_platform_firmware	1037
	snapdragon_wear_4100\+_platform_firmware	1037
	snapdragon_x12_lte_modem_firmware	1038
	snapdragon_x20_lte_modem_firmware	1038
	snapdragon_x24_lte_modem_firmware	1038
	snapdragon_x50_5g_modem- rf_system_firmware	1039
	snapdragon_x55_5g_modem- rf_system_firmware	1039
	snapdragon_x5_lte_modem_firmware	1040
	snapdragon_x65_5g_modem- rf_system_firmware	1040
Qualacture	snapdragon_xr1_platform_firmware	1040
Qualcomm	snapdragon_xr2\+_gen_1_platform_firmware	1041
	snapdragon_xr2_5g_platform_firmware	1041
	ssm7250-aa_firmware	1042
	sw5100p_firmware	1042
	sw5100_firmware	1042
	sxr1120_firmware	1043
	sxr2130_firmware	1043
	wcd9326_firmware	1043
	wcd9330_firmware	1044
	wcd9335_firmware	1044
	wcd9340_firmware	1045
	wcd9341_firmware	1045
	wcd9370_firmware	1046
	wcd9371_firmware	1046
	wcd9375_firmware	1047
	wcd9380_firmware	1047

Vendor	Product	Page Number
	wcd9385_firmware	1047
	wcn3610_firmware	1048
	wcn3615_firmware	1048
	wcn3620_firmware	1049
	wcn3660b_firmware	1049
	wcn3660_firmware	1050
	wcn3680b_firmware	1050
	wcn3680_firmware	1051
	wcn3910_firmware	1051
	wcn3950_firmware	1051
	wcn3980_firmware	1052
Qualcomm	wcn3988_firmware	1052
	wcn3990_firmware	1053
	wcn3998_firmware	1053
	wcn3999_firmware	1054
	wcn6740_firmware	1054
	wcn6750_firmware	1054
	wcn685x-1_firmware	1055
	wcn685x-5_firmware	1055
	wsa8810_firmware	1056
	wsa8815_firmware	1056
	wsa8830_firmware	1056
	wsa8835_firmware	1057
Redhat	enterprise_linux	1057
Rockwellautomation	armorstart_st_281e_firmware	1060
NULKWEIIAULUIIIAUIUII	armorstart_st_284ee_firmware	1067
	android	1074
	exynos_1080_firmware	1088
Samsung	exynos_5123_firmware	1088
	exynos_5300_firmware	1089
	exynos_980_firmware	1089
shapeshift	keepkey_firmware	1090

Vendor	Product	Page Number
	6gk1411-1ac00_firmware	1090
Siemens	6gk1411-5ac00_firmware	1095
	scalance_lpe9403_firmware	1099
spryker	commerce_os	1101
Tenda	ac18_firmware	1101
	n301_firmware	1102
totolink	a7100ru_firmware	1103
	x5000r_firmware	1103
Zyxel	nbg-418n_firmware	1104
Цулсі	nbg6604_firmware	1106

	Common Vu	Inerabi	lities and Exposure	es (CVE) Rej	port
Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
	l		Application		
Vendor: 8w	eb				
Product: rea	ad_more_withou	ıt_refresh	ľ		
Affected Ver	sion(s): * Up to (	excluding)	3.2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Eightweb Interactive Read More Without Refresh plugin <= 3.1 versions. <b>CVE ID : CVE-2023- 23793</b>	N/A	A-8WE-READ- 170523/1
Vendor: 9se	eds			I	
Product: cp	tspeakers				
Affected Ver	sion(s): * Up to (i	ncluding)	1.1		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in 9seeds.Com CPT – Speakers plugin <= 1.1 versions. CVE ID : CVE-2023- 25977	N/A	A-9SE-CPT 170523/2
	vancedcustomfi	elds			
	vanced_custom				
			5.0.0 Up to (excluding) 5	.12.5	
Deserializa tion of Untrusted Data	02-May-2023	8.8	The Advanced Custom Fields (ACF) Free and Pro WordPress plugins 6.x before 6.1.0 and 5.x before 5.12.5 unserialize user controllable data,	N/A	A-ADV-ADVA- 170523/3

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): From (in	cluding) 6	which could allow users with a role of Contributor and above to perform PHP Object Injection when a suitable gadget is present. <b>CVE ID : CVE-2023-</b> <b>1196</b>	.1.0	
			The Advanced		
Deserializa tion of Untrusted Data	02-May-2023	8.8	Custom Fields (ACF) Free and Pro WordPress plugins 6.x before 6.1.0 and 5.x before 5.12.5 unserialize user controllable data, which could allow users with a role of Contributor and above to perform PHP Object Injection when a suitable gadget is present. <b>CVE ID : CVE-2023-</b>	N/A	A-ADV-ADVA- 170523/4
			1196		
Vendor: age	entevolution				
	press_listings				
Affected Ver	sion(s): * Up to (i	including)		1	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Agent Evolution IMPress Listings plugin <= 2.6.2 versions. <b>CVE ID : CVE-2023-</b> <b>22711</b>	N/A	A-AGE-IMPR- 170523/5

0-1

1-2

2-3

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: agi	lepoint				I
Product: ag	ilepoint_nx				
Affected Ver	sion(s): 8.0				
Unrestricte d Upload of File with Dangerous Type	08-May-2023	9.8	AgilePoint NX v8.0 SU2.2 & SU2.3 – Insecure File Upload - Vulnerability allows insecure file upload, by an unspecified request. <b>CVE ID : CVE-2023-</b>	N/A	A-AGI-AGIL- 170523/6
N/A	08-May-2023	9.1	24507 AgilePoint NX v8.0 SU2.2 & SU2.3 – Arbitrary File Delete Vulnerability allows arbitrary file deletion, by an unspecified request. CVE ID : CVE-2023- 31178	N/A	A-AGI-AGIL- 170523/7
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-May-2023	7.5	AgilePoint NX v8.0 SU2.2 & SU2.3 - Path traversal - Vulnerability allows path traversal and downloading files from the server, by an unspecified request.	N/A	A-AGI-AGIL- 170523/8

0-1

1-2

2-3

5-6 6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 31179		
Vendor: Am	azon				
Product: op	ensearch				
Affected Ver	sion(s): * Up to (	excluding)	1.3.10		
Incorrect Authorizati on	08-May-2023	5.9	OpenSearch is open- source software suite for search, analytics, and observability applications. Prior to versions 1.3.10 and 2.7.0, there is an issue with the implementation of fine-grained access control rules (document-level security, field-level security and field masking) where they are not correctly applied to the queries during extremely rare race conditions potentially leading to incorrect access authorization. For this issue to be triggered, two concurrent requests need to land on the same instance exactly when query cache eviction happens, once every four hours. OpenSearch 1.3.10 and 2.7.0 contain a fix for this issue.	https://githu b.com/opens earch- project/secu rity/security /advisories/ GHSA-g8xc- 6mf7-h28h	A-AMA-OPEN- 170523/9

0-1

1-2

2-3

**3-4 4-5** Page **4** of **1106**  6-7 7-8

5-6

0-1

1-2

2-3

**3-4 4-5** Page **5** of **1106**  6-7 7-8

5-6

Affected Version(s): * Up to (excluding) 1.3.10         OpenSearch is open- source software suite for search, analytics, and observability applications. Prior to versions 1.3.10 and 2.7.0, there is an issue with the implementation of fine-grained access control rules (document-level security and field masking) where they are not correctly applied to the queries during extremely rare race conditions potentially leading to incorrect access authorization. For this issue to be triggered, two concurrent requests need to land on the same instance exactly when query cache eviction happens, once every four hours. OpenSearch 1.3.10 and 2.7.0 contain a fix for this issue.       A-AMA-OPEN- 170523/11	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Incorrect Authorizatio on08-May-20235.95.9source software suite for search, analytics, and observability applications. Prior to versions 1.3.10 and 2.7.0, there is an issue with the implementation of fine-grained access control rules (document-level security, field-level security and field masking) where they applied to the queries during extremely rare race conditions potentially leading to incorrect access authorization. For this issue to be triggered, two concurrent requests need to land on the same instance exactly when query cache eviction happens, once every four hours. OpenSearch 1.3.10 and 2.7.0 contain a fix for this issue.https://githu b.com/opens earch- project/secu rity/security /divisories/ GHSA-g8xc- 6mf7-h28hA-AMA-OPEN- 170523/11	Affected Vers	Affected Version(s): * Up to (excluding) 1.3.10						
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.7.0	Authorizati on			source software suite for search, analytics, and observability applications. Prior to versions 1.3.10 and 2.7.0, there is an issue with the implementation of fine-grained access control rules (document-level security, field-level security and field masking) where they are not correctly applied to the queries during extremely rare race conditions potentially leading to incorrect access authorization. For this issue to be triggered, two concurrent requests need to land on the same instance exactly when query cache eviction happens, once every four hours. OpenSearch 1.3.10 and 2.7.0 contain a fix for this issue. <b>CVE ID : CVE-2023- 31141</b>	b.com/opens earch- project/secu rity/security /advisories/ GHSA-g8xc- 6mf7-h28h			

0-1

1-2

2-3

3-4 4-5 Page 6 of 1106

7-8 8-9 9-10

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorizati on	08-May-2023 <b>r-ical-events-lis</b>	5.9	OpenSearch is open- source software suite for search, analytics, and observability applications. Prior to versions 1.3.10 and 2.7.0, there is an issue with the implementation of fine-grained access control rules (document-level security, field-level security, field-level security and field masking) where they are not correctly applied to the queries during extremely rare race conditions potentially leading to incorrect access authorization. For this issue to be triggered, two concurrent requests need to land on the same instance exactly when query cache eviction happens, once every four hours. OpenSearch 1.3.10 and 2.7.0 contain a fix for this issue. <b>CVE ID : CVE-2023- 31141</b>	https://githu b.com/opens earch- project/secu rity/security /advisories/ GHSA-g8xc- 6mf7-h28h	A-AMA-OPEN- 170523/12
	r-ical-events-lis				
	sion(s): * Up to (i		6.6		
Ameeteu vers		nendulligj	0.0		

0-1

1-2

2-3

**3-4 4-5** Page **7** of **1106**  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')	02-May-2023	4.8	The amr ical events lists WordPress plugin through 6.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) CVE ID : CVE-2023- 1021	N/A	A-AMR-AMR 170523/13
Vendor: ans	swer				
Product: an	swer				
Affected Vers	sion(s): * Up to (e	excluding)	1.0.9		
Missing Authorizati on	09-May-2023	3.5	Missing Authorization in GitHub repository answerdev/answer prior to 1.0.9. <b>CVE ID : CVE-2023- 2590</b>	https://hunt r.dev/bounti es/a4238a3 0-3ddb- 4415-9055- e179c3d4de a7, https://githu b.com/answ erdev/answ er/commit/ 51ac1e6b76 ae9ab3ca20 08ca4819c0 cc3bd2fcd3	A-ANS-ANSW- 170523/14
	abot_white-jott		t		
	tabot_white-jot	ter			
	sion(s): 0.2.2				
Unrestricte d Upload of	01-May-2023	9.8	File upload vulnerability in	https://githu b.com/Antab	A-ANT-ANTA- 170523/15
CVSS Scoring S	Scale 0-1 C	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>8</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			Antabot White-Jotter v0.2.2, allows remote attackers to execute malicious code via the file parameter to function coversUpload. <b>CVE ID : CVE-2023-</b> <b>29635</b>	ot/White- Jotter/issues /157, https://githu b.com/Antab ot/White- Jotter/blob/ c1c5d66fda0 90b986b8f4 6a7132d403 e3b038c5d/ wj/src/main /java/com/g m/wj/contro ller/Library Controller.ja va#L63	
Vendor: Apa	ache				
Product: air	rflow				
Affected Ver	sion(s): * Up to (e	excluding)	2.6.0		
N/A	08-May-2023	9.8	Privilege Context Switching Error vulnerability in Apache Software Foundation Apache Airflow.This issue affects Apache Airflow: before 2.6.0.	https://githu b.com/apach e/airflow/pu ll/29506	A-APA-AIRF- 170523/16
			CVE ID : CVE-2023- 25754		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	Task instance details page in the UI is vulnerable to a stored XSS.This issue affects Apache Airflow: before 2.6.0.	https://githu b.com/apach e/airflow/pu ll/30779, https://githu b.com/apach e/airflow/pu ll/30447	A-APA-AIRF- 170523/17

0-1

1-2

2-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29247		
Product: br	рс				
Affected Ver	sion(s): From (in	cluding) (	.9.0 Up to (excluding) 1	.5.0	
Improper Input Validation	08-May-2023	9.8	Security vulnerability in Apache bRPC <1.5.0 on all platforms allows attackers to execute arbitrary code via ServerOptions::pid_fi le. An attacker that can influence the ServerOptions pid_file parameter with which the bRPC server is started can execute arbitrary code with the permissions of the bRPC process. Solution: 1. upgrade to bRPC >= 1.5.0, download link: https://dist.apa che.org/repos/dist/r elease/brpc/1.5.0/ https://dist.apache.o rg/repos/dist/releas e/brpc/1.5.0/ 2. If you are using an old version of bRPC and hard to upgrade, you can apply this patch: https://githu b.com/apache/brpc/ pull/2218	https://lists. apache.org/t hread/jqpttr qbc38yhckg p67xk399hq xnz7jn, http://www. openwall.co m/lists/oss- security/202 3/05/08/1	A-APA-BRPC- 170523/18

0-1

1-2

2-33-44-5Page 10 of 1106

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			https://github.com/ apache/brpc/pull/2 218		
			CVE ID : CVE-2023- 31039		
Product: co	uchdb			<u> </u>	
Affected Ver	sion(s): * Up to (	excluding)	3.2.3		
N/A	02-May-2023	5.3	Design documents with matching document IDs, from databases on the same cluster, may share a mutable Javascript environment when using these design document functions: * validate_doc_update * list * filter * filter views (using view functions as filters) * rewrite * update This doesn't affect map/reduce or	https://docs. couchdb.org /en/stable/c ve/2023- 26268.html	A-APA-COUC- 170523/19

CVSS	Scoring	Scale
------	---------	-------

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			search (Dreyfus) index functions.		
			Users are recommended to upgrade to a version that is no longer affected by this issue (Apache CouchDB 3.3.2 or 3.2.3).		
			Workaround: Avoid using design documents from untrusted sources which may attempt to cache or store data in the Javascript environment.		
		1 1	CVE ID : CVE-2023- 26268	2.2	
Affected Ver	sion(s): From (in	cluding) 3	.3.0 Up to (excluding) 3	.3.2	
N/A	02-May-2023	5.3	Design documents with matching document IDs, from databases on the same cluster, may share a mutable Javascript environment when using these design document functions: * validate_doc_update * list	https://docs. couchdb.org /en/stable/c ve/2023- 26268.html	A-APA-COUC- 170523/20

0-1

1-2

2-33-44-5Page 12 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* filter		
			* filter views (using view functions as filters)		
			* rewrite		
			* update		
			This doesn't affect map/reduce or search (Dreyfus) index functions.		
			Users are recommended to upgrade to a version that is no longer affected by this issue (Apache CouchDB 3.3.2 or 3.2.3).		
			Workaround: Avoid using design documents from untrusted sources which may attempt to cache or store data in the Javascript environment.		
			CVE ID : CVE-2023- 26268		
Product: log	g4cxx				1
CVSS Scoring S	Scale 0-1	L-2 2-3	<b>3-4 4-5 5-6</b> Page <b>13</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Page 13 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): From (in	cluding) 0	.9.0 Up to (excluding) 1	.1.0	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	08-May-2023	8.8	SQL injection in Log4cxx when using the ODBC appender to send log messages to a database. No fields sent to the database were properly escaped for SQL injection. This has been the case since at least version 0.9.0(released 2003- 08-06) Note that Log4cxx is a C++ framework, so only C++ applications are affected. Before version 1.1.0, the ODBC appender was automatically part of Log4cxx if the library was found when compiling the library. As of version 1.1.0, this must be both explicitly enabled in order to be compiled in.	https://lists. apache.org/t hread/vgjlpd f353vv91gry spwxrzj6p0f bjd9	A-APA-LOG4- 170523/21

0-1

1-2

2-3

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Three preconditions must be met for this vulnerability to be possible:		
			1. Log4cxx compiled with ODBC support(before version 1.1.0, this was auto-detected at compile time)		
			2. ODBCAppender enabled for logging messages to, generally done via a config file		
			3. User input is logged at some point. If your application does not have user input, it is unlikely to be affected.		
			Users are recommended to upgrade to version 1.1.0 which properly binds the parameters to the SQL statement, or migrate to the new DBAppender class which supports an ODBC connection		

0-1

1-2

2-33-44-5Page 15 of 1106

5-6

6-7

7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in addition to other databases. Note that this fix does require a configuration file update, as the old configuration files will not configure properly. An example is shown below, and more information may be found in the Log4cxx documentation on the ODBCAppender.		
			Example of old configuration snippet: <appender name="SqlODBCApp ender" class="ODBCAppend er"&gt;</appender 		
			<param name="sql" value="INSERT INTO logs (message) VALUES ('%m')" /&gt;  other params here</param 		

0-1

1-2

2-33-44-5Page 16 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The migrated configuration snippet with new ColumnMapping parameters:		
			<appender name="SqlODBCApp ender" class="ODBCAppend er"&gt;</appender 		
			<param name="sql" value="INSERT INTO logs (message) VALUES (?)" /&gt;</param 		
			<param name="ColumnMapp ing" value="message"/&gt;  other params here</param 		

0-1

1-2

2-33-44-5Page 17 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 31038		
Product: sp					
Affected Ver	<mark>sion(s): * Up to (i</mark>	nciuding)	3.0.3 ** UNSUPPORTED		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	02-May-2023	8.8	WHEN ASSIGNED ** The Apache Spark UI offers the possibility to enable ACLs via the configuration option spark.acls.enable. With an authentication filter, this checks whether a user has access permissions to view or modify the application. If ACLs are enabled, a code path in HttpSecurityFilter can allow someone to perform impersonation by providing an arbitrary user name. A malicious user might then be able to reach a permission check function that will ultimately build a Unix shell command based on their input, and execute it. This will	https://spar k.apache.org /security.ht ml	A-APA-SPAR- 170523/22

0-1

1-2

2-3

6-7

7-8

5-6

Weakness	Publish Date	CVSSv	3	Descripti	on & CVE	ID		Patch		NC	IIPC ID	
				result in a shell com execution Spark is c running a ssue was earlier as 33891, bu ncorrect version 3 nas since would no affected.	mand a as the u currently is. This disclos CVE-20 at ly claime .1.3 (wh gone EC	user y ed 22- ed iich						
				NOTE: Th vulnerabi affects pr are no lor supporte maintaine	ility only oducts t 1ger d by the	hat						
			] ] [ ]	Users are recomme upgrade t supporte Apache S as version	nded to to a d versio park, su	n of						
			3	CVE ID : ( 32007								
Affected Ver	<mark>sion(s): From (in</mark>	cluding	-	.1 Up to ** UNSUF			1.3					
Neutralizat ion of Special Elements used in a Command ('Comman	02-May-2023	8.8		WHEN AS The Apac offers the to enable the configoption spark.acls	he Sparl possibi ACLs vi guration	k UI lity a	k.aj	ps://sj pache. curity	org	A-APA 17052		
						1		67	7.0			
CVSS Scoring S	Scale 0-1	L-2	2-3	3-4	4-5	5-6		6-7	7-8	8 8-9	9-10	

Page **19** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			With an authentication filter, this checks whether a user has access permissions to view or modify the application. If ACLs are enabled, a code path in HttpSecurityFilter can allow someone to perform impersonation by providing an arbitrary user name. A malicious user might then be able to reach a permission check function that will ultimately build a Unix shell command based on their input, and execute it. This will result in arbitrary shell command execution as the user Spark is currently running as. This issue was disclosed earlier as CVE-2022- 33891, but incorrectly claimed version 3.1.3 (which has since gone EOL) would not be affected.		
			NOTE: This vulnerability only affects products that are no longer		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supported by the maintainer.		
			Users are recommended to upgrade to a supported version of Apache Spark, such as version 3.4.0.		
Affected Ver	sion(s): From (in	cluding) 3	CVE ID : CVE-2023- 32007 .2.0 Up to (including) 3	2.1	
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	02-May-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** The Apache Spark UI offers the possibility to enable ACLs via the configuration option spark.acls.enable. With an authentication filter, this checks whether a user has access permissions to view or modify the application. If ACLs are enabled, a code path in HttpSecurityFilter can allow someone to perform impersonation by providing an arbitrary user name. A malicious user might then be able to reach a permission	https://spar k.apache.org /security.ht ml	A-APA-SPAR- 170523/24

0-1

1-2

2-33-44-5Page 21 of 1106

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	Description & CVE ID check function that will ultimately build a Unix shell command based on their input, and execute it. This will result in arbitrary shell command execution as the user Spark is currently running as. This issue was disclosed earlier as CVE-2022- 33891, but incorrectly claimed version 3.1.3 (which has since gone EOL) would not be affected. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	Patch	NCIIPC ID
			Users are recommended to upgrade to a supported version of Apache Spark, such as version 3.4.0.		
Vendor: appin	m		CVE ID : CVE-2023- 32007		
Product: appi	um-desktop				

0-1

1-2

2-3

6-7 7-8

5-6

	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): * Up to (	excluding)	1.22.3-4		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	02-May-2023	9.8	OS Command Injection in GitHub repository appium/appium- desktop prior to v1.22.3-4. <b>CVE ID : CVE-2023-</b> <b>2479</b>	https://hunt r.dev/bounti es/fbdeec3c- d197-4a68- a547- 7f93fb9594b 4, https://githu b.com/appiu m/appium- desktop/co mmit/12a98 8aa08b9822 e97056a094 86c9bebb3a ad8fe	A-APP-APPI- 170523/25
Vendor: App	ple				
Product: saf	fari				
Affected Vers	sion(s): * Up to (	excluding)	16.4		
N/A	08-May-2023	9.8	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A remote user may be able to cause unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 28201</b>	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 6	A-APP-SAFA- 170523/26
				0	

Page 23 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information <b>CVE ID : CVE-2023- 27954</b>	m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
Product: xc	ode				
Affected Ver	sion(s): * Up to (e	excluding)	14.3		
N/A	08-May-2023	8.6	The issue was addressed with improved memory handling. This issue is fixed in Xcode 14.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges	https://supp ort.apple.co m/en- us/HT21367 9	A-APP-XCOD- 170523/28

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 27967		
N/A	08-May-2023	6.3	This issue was addressed with improved entitlements. This issue is fixed in Xcode 14.3. A sandboxed app may be able to collect system logs <b>CVE ID : CVE-2023-</b> <b>27945</b>	https://supp ort.apple.co m/en- us/HT21367 9	A-APP-XCOD- 170523/29
Vendor: arc	herirm				
Product: ar	cher				
Affected Ver	sion(s): From (in	cluding) 6	5.12.0.0 Up to (excluding	g) 6.12.0.6.1	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	01-May-2023	5.4	Archer Platform 6.8 before 6.12 P6 HF1 (6.12.0.6.1) contains a stored XSS vulnerability. A remote authenticated malicious Archer user could potentially exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. 6.11.P4 (6.11.0.4) is also a fixed release. <b>CVE ID : CVE-2023-</b> <b>30639</b>	https://ww w.archerirm. community/ t5/security- advisories/a rcher- update-for- stored-cross- site- scripting/ta- p/697581	A-ARC-ARCH- 170523/30
Affected Ver	sion(s): From (in	cluding) 6	.8.0.0 Up to (including)	6.11.0.4	l
Improper Neutralizat ion of Input	01-May-2023	5.4	Archer Platform 6.8 before 6.12 P6 HF1 (6.12.0.6.1) contains a stored XSS	https://ww w.archerirm. community/ t5/security-	A-ARC-ARCH- 170523/31

0-1

1-2

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')			vulnerability. A remote authenticated malicious Archer user could potentially exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. 6.11.P4 (6.11.0.4) is also a fixed release.	advisories/a rcher- update-for- stored-cross- site- scripting/ta- p/697581	
			CVE ID : CVE-2023- 30639		
Vendor: art	isanworkshop			I	
Product: jap	panized_for_woo	commer	ce		
Affected Ver	sion(s): * Up to (e	excluding)	2.5.8		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	6.1	The Japanized For WooCommerce WordPress plugin before 2.5.8 does not escape generated URLs before outputting them in attributes, leading to Reflected Cross-Site Scripting CVE ID : CVE-2023- 0948	N/A	A-ART-JAPA- 170523/32
Vendor: asn	nbb_project				
Product: as					
	sion(s): 2.9.1				
Improper Neutralizat ion of Input During Web Page Generation	08-May-2023	6.1	AsmBB v2.9.1 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities via the MiniMag.asm	https://asm 32.info/fossi l/asmbb/inf o/7dfa4f56b 473f76c, https://fresh .flatassemble	A-ASM-ASMB- 170523/33
CVSS Scoring S	Scale 0-1	1-2 2-3		6-7 7-8	8 8-9 9-10
			Page <b>26</b> of <b>1106</b>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			and bbcode.asm libraries. CVE ID : CVE-2023- 30334	r.net/fossil/r epo/fresh/in fo/a3caaf7a d8503348	
Vendor: Atl	assian			L	
Product: co	nfluence_data_c	enter			
Affected Ver	sion(s): * Up to (	excluding)		r	
N/A Affected Ver	01-May-2023	5.3	Affected versions of Atlassian Confluence Server and Data Center allow anonymous remote attackers to view the names of attachments and labels in a private Confluence space. This occurs via an Information Disclosure vulnerability in the macro preview feature. This vulnerability was reported by Rojan Rijal of the Tinder Security Engineering team. The affected versions are before version 7.13.15, from version 7.14.0 before 7.19.7, and from version 7.20.0 before 8.2.0. <b>CVE ID : CVE-2023- 22503</b>	https://jira.a tlassian.com /browse/CO NFSERVER- 82403	A-ATL-CONF- 170523/34

0-1

1-2

2-33-44-5Page 27 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
N/A	01-May-2023	5.3	Affected versions of Atlassian Confluence Server and Data Center allow anonymous remote attackers to view the names of attachments and labels in a private Confluence space. This occurs via an Information Disclosure vulnerability in the macro preview feature. This vulnerability was reported by Rojan Rijal of the Tinder Security Engineering team. The affected versions are before version 7.13.15, from version 7.14.0 before 7.19.7, and from version 7.20.0 before 8.2.0. <b>CVE ID : CVE-2023- 22503</b>	https://jira.a tlassian.com /browse/CO NFSERVER- 82403	A-ATL-CONF- 170523/35					
Affected Ver	sion(s): From (in	cluding) 7	2.20.0 Up to (excluding)	8.2.0						
N/A	01-May-2023	5.3	Affected versions of Atlassian Confluence Server and Data Center allow anonymous remote attackers to view the names of attachments and labels in a private Confluence space.	https://jira.a tlassian.com /browse/CO NFSERVER- 82403	A-ATL-CONF- 170523/36					
CVSS Scoring				6.7 70	8.0 0.10					
CV35 SCOTINg		2-3	Page <b>28</b> of <b>1106</b>	CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10						

Page 28 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This occurs via an Information Disclosure vulnerability in the macro preview feature.		
			This vulnerability was reported by Rojan Rijal of the Tinder Security Engineering team.		
			The affected versions are before version 7.13.15, from version 7.14.0 before 7.19.7, and from version 7.20.0 before 8.2.0.		
			CVE ID : CVE-2023- 22503		
	nfluence_server				
Affected Ver	sion(s): * Up to (e	excluding)		ſ	
N/A	01-May-2023	5.3	Affected versions of Atlassian Confluence Server and Data Center allow anonymous remote attackers to view the names of attachments and labels in a private Confluence space. This occurs via an Information Disclosure vulnerability in the macro preview feature.	https://jira.a tlassian.com /browse/CO NFSERVER- 82403	A-ATL-CONF- 170523/37

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability was reported by Rojan Rijal of the Tinder Security Engineering team.		
			The affected versions are before version 7.13.15, from version 7.14.0 before 7.19.7, and from version 7.20.0 before 8.2.0.		
			CVE ID : CVE-2023- 22503		
Affected Ver	sion(s): From (in	cluding) 7	.14.0 Up to (excluding)	7.19.7	
N/A	01-May-2023	5.3	Affected versions of Atlassian Confluence Server and Data Center allow anonymous remote attackers to view the names of attachments and labels in a private Confluence space. This occurs via an Information Disclosure vulnerability in the macro preview feature.	https://jira.a tlassian.com /browse/CO NFSERVER- 82403	A-ATL-CONF- 170523/38
			This vulnerability was reported by Rojan Rijal of the Tinder Security Engineering team.		
			The affected versions are before version 7.13.15, from version		

0-1

1-2

2-33-44-5Page 30 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			7.14.0 before 7.19.7, and from version 7.20.0 before 8.2.0.				
			CVE ID : CVE-2023- 22503				
Affected Ver	sion(s): From (in	cluding) 7	.20.0 Up to (excluding)	8.2.0			
Affected Version(s): From (including) 7.20.0 Up to (excluding) 8.2.0N/AAffected versions of Atlassian Confluence Server and Data Center allow anonymous remote attachments and labels in a private Confluence space. This occurs via an Information 							
		king one	<b>n</b> 0				
	tels_online_bool	0 0					
Allected ver	sion(s): * Up to (i	nciuuliigj	5.0.5				

0-1

1-2

2-3

**3-4 4-5** Page **31** of **1106**  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')	08-May-2023	8.8	The Avirato hotels online booking engine WordPress plugin through 5.0.5 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. <b>CVE ID : CVE-2023-</b> 0768	N/A	A-AVI-HOTE- 170523/40
Vendor: azu	ıracast			<u> </u>	
Product: az	uracast				
Affected Ver	sion(s): * Up to (e	excluding)	0.18.3		
Improper Restriction of Excessive Authentica tion Attempts	05-May-2023	9.8	Improper Restriction of Excessive Authentication Attempts in GitHub repository azuracast/azuracast prior to 0.18.3. <b>CVE ID : CVE-2023- 2531</b>	https://hunt r.dev/bounti es/20463eb 2-0f9d-4ea3- a2c8- 93f80e7aca0 2, https://githu b.com/azura cast/azuraca st/commit/b db23594ad3 e0c47c8568 ce028a7c24 4a406cf9d	A-AZU-AZUR- 170523/41
Vendor: bas	ixonline			·	·
Product: ne					
Affected Ver	sion(s): * Up to (e	excluding)			1
Improper Neutralizat ion of	08-May-2023	7.2	The NEX-Forms WordPress plugin before 8.4 does not	N/A	A-BAS-NEX 170523/42
CVSS Scoring S	Scale 0-1 :	L-2 <u>2-</u> 3	<b>3-4 4-5 5-</b> 0 Page <b>32</b> of <b>1106</b>	6 6-7 7-8	8 8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL			properly escape the `table` parameter, which is populated with user input, before concatenating it to an SQL query.		
Injection')			CVE ID : CVE-2023- 2114		
Vendor: bee	etl_project			<u> </u>	
Product: be	etl				
Affected Ver	sion(s): 3.15				
N/A	04-May-2023	9.8	An issue in the render function of beetl v3.15.0 allows attackers to execute server-side template injection (SSTI) via a crafted payload.	N/A	A-BEE-BEET- 170523/43
			CVE ID : CVE-2023- 30331		
Vendor: bill	ling_manageme	nt_system	_project		
Product: bil	lling_manageme	ent_system	n		
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	09-May-2023	9.8	A vulnerability has been found in SourceCodester Billing Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file ajax_service.php of the component POST Parameter Handler. The manipulation of the argument drop_services leads to sql injection. The	N/A	A-BIL-BILL- 170523/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-228397 was assigned to this vulnerability.		
			CVE ID : CVE-2023- 2595		
Vendor: bin	g_site_verificati	on_plugir	n_using_meta_tag_proj	ect	
	0		n_using_meta_tag		
Affected Vers	sion(s): * Up to (i	including)		1	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Himanshu Bing Site Verification plugin using Meta Tag plugin <= 1.0 versions.	N/A	A-BIN-BING- 170523/45
	alvan dauhita digi	tal	CVE ID : CVE-2023- 23875		
Product: tre	ckandwhitedigi				
	sion(s): * Up to (e	evcluding	300		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Black and White Digital Ltd TreePress – Easy Family Trees & Ancestor Profiles plugin <= 2.0.22 versions. <b>CVE ID : CVE-2023-</b>	N/A	A-BLA-TREE- 170523/46
			23863		

0-1

1-2

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: blu	eglass	I		I	
Product: joł	os_for_wordpres	s			
Affected Ver	sion(s): * Up to (e	excluding)	2.5.11		
Improper Neutralizat ion of Input During Web Page Generation	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in BlueGlass Jobs for WordPress plugin <= 2.5.10.2 versions.	N/A	A-BLU-JOBS- 170523/47
('Cross-site Scripting')			CVE ID : CVE-2023- 26017		
Vendor: boo	oqable				
Product: re	ntal_software_b	ooqable_i	rental		
Affected Ver	sion(s): * Up to (i	ncluding)	2.4.15		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Booqable Rental Software Booqable Rental plugin <= 2.4.15 versions. CVE ID : CVE-2023- 30746	N/A	A-BOO-RENT- 170523/48
Vendor: bui	nsys_project				
Product: bu	msys				
Affected Ver	sion(s): * Up to (e	excluding)	2.1.1		
Inclusion of Functionali ty from Untrusted Control Sphere	05-May-2023	8.8	PHP Remote File Inclusion in GitHub repository unilogies/bumsys prior to 2.1.1. <b>CVE ID : CVE-2023- 2551</b>	https://githu b.com/unilo gies/bumsys /commit/86 e29dd23df3 48ec6075f0c 0de8e06b8d 9fb0a9a, https://hunt r.dev/bounti es/5723613	A-BUM-BUMS- 170523/49

0-1

1-2

2-3

**3-4 4-5** Page **35** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				c-55c6-4f18- 9ed3- 61ad44f5de 9c	
Cross-Site Request Forgery (CSRF)	05-May-2023	8.8	Cross-Site Request Forgery (CSRF) in GitHub repository unilogies/bumsys prior to 2.1.1. <b>CVE ID : CVE-2023-</b> <b>2552</b>	https://hunt r.dev/bounti es/ab0b465 5-f57a-4113- 849b- 2237eeb75b 32, https://githu b.com/unilo gies/bumsys /commit/86 e29dd23df3 48ec6075f0c 0de8e06b8d 9fb0a9a	A-BUM-BUMS- 170523/50
Affected Version(s): * Up to (excluding) 2.2.0					
External Control of File Name or Path	05-May-2023	7.2	External Control of File Name or Path in GitHub repository unilogies/bumsys prior to 2.2.0. <b>CVE ID : CVE-2023- 2554</b>	https://hunt r.dev/bounti es/396785a 0-7bb6- 4db4-b4cb- 607b0fd4ab 4b, https://githu b.com/unilo gies/bumsys /commit/1b 426f58a513 194206d0ea 8ab58baf14 61e54978	A-BUM-BUMS- 170523/51
Improper Neutralizat ion of Input During Web Page Generation	05-May-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository unilogies/bumsys prior to 2.2.0. CVE ID : CVE-2023- 2553	https://hunt r.dev/bounti es/4e1f5b56 -e846-40d8- a83c- 533efd56aac f, https://githu	A-BUM-BUMS- 170523/52

2-3 Page **36** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')				b.com/unilo gies/bumsys /commit/1b 426f58a513 194206d0ea 8ab58baf14 61e54978	
Vendor: byc	console				
Product: pie	ckup_\ _delivery	/_\ _dine-	in_date_time		
Affected Ver	sion(s): * Up to (i	ncluding)	1.0.9		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	4.8	The Pickup   Delivery   Dine-in date time WordPress plugin through 1.0.9 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) <b>CVE ID : CVE-2023- 0894</b>	N/A	A-BYC-PICK- 170523/53
Vendor: cat	chthemes			I	
Product: da	rcie				
Affected Ver	sion(s): * Up to (e	excluding)	1.1.6		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Catch Themes Darcie theme <= 1.1.5 versions. <b>CVE ID : CVE-2023- 25961</b>	N/A	A-CAT-DARC- 170523/54
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5-6	6-7 7-8	<u> </u>
			Page <b>37</b> of <b>1106</b>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: cat	ontechnology			<u> </u>	
Product: ca	ton_prime				
Affected Ver	sion(s): 2.1.2.51.	e8d72250	49\\(202303031001\\	)	
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	04-May-2023	9.8	A vulnerability was found in Caton Prime 2.1.2.51.e8d7225049 (202303031001) and classified as critical. This issue affects some unknown processing of the file cgi- bin/tools_ping.cgi?ac tion=Command of the component Ping Handler. The manipulation of the argument Destination leads to command injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB- 228011. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. <b>CVE ID : CVE-2023- 2520</b>	N/A	A-CAT-CATO- 170523/55
Affected Ver Improper	sion(s): 1.2.9		A vulnerability has		
Neutralizat ion of Special Elements used in an SQL	04-May-2023	9.8	been found in Caton CTP Relay Server 1.2.9 and classified as critical. This vulnerability affects unknown code of the	N/A	A-CAT-CTP 170523/56
CVSS Scoring S	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')			file /server/api/v1/logi n of the component API. The manipulation of the argument username/password leads to sql injection. The attack can be initiated remotely. VDB-228010 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. <b>CVE ID : CVE-2023-</b>		
			2519		
Vendor: Ces	anta				
Product: mj	S				
Affected Ver	sion(s): 1.26				
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-May-2023	5.5	An issue found in Cesanta MJS v.1.26 allows a local attacker to cause a denial of service via the mjs_execute function in mjs.c. <b>CVE ID : CVE-2023-</b> <b>30088</b>	https://githu b.com/cesan ta/mjs/issue s/243	A-CES-MJS- 170523/57
Vendor: Cha	amilo				
Product: ch	amilo_lms				
Affected Ver	sion(s): 1.11.18				
Improper Neutralizat ion of Input During Web Page	09-May-2023	6.1	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary	https://supp ort.chamilo.o rg/projects/ chamilo- 18/wiki/Sec urity_issues	A-CHA-CHAM- 170523/58
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5-6	6-7 7-8	<u> </u>
			Page <b>39</b> of <b>1106</b>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			code via the skills wheel parameter. CVE ID : CVE-2023- 31801	#Issue-97- 2023-04-11- Low-impact- High-risk- XSS-in-skills- wheel	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the forum title parameter. CVE ID : CVE-2023- 31800	https://supp ort.chamilo.o rg/projects/ chamilo- 18/wiki/Sec urity_issues #Issue-102- 2023-04-11- Low-impact- Moderate- risk-XSS-in- forum-titles	A-CHA-CHAM- 170523/59
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the skype and linedin_url parameters. CVE ID : CVE-2023- 31802	https://supp ort.chamilo.o rg/projects/ chamilo- 18/wiki/Sec urity_issues #Issue-104- 2023-04-11- Moderate- impact-High- risk-XSS-in- personal- profile	A-CHA-CHAM- 170523/60
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the course category parameters. <b>CVE ID : CVE-2023-</b> <b>31804</b>	https://supp ort.chamilo.o rg/projects/ chamilo- 18/wiki/Sec urity_issues #Issue-96- 2023-04-06- Low-impact- Moderate- risk-XSS-in-	A-CHA-CHAM- 170523/61

0-1

1-2

2-33-44-5Page 40 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				course- categories	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via a crafted payload to the My Progress function. <b>CVE ID : CVE-2023-</b> <b>31806</b>	https://supp ort.chamilo.o rg/projects/ chamilo- 18/wiki/Sec urity_issues #Issue-103- 2023-04-11- Low-impact- Moderate- risk-XSS-in- My- progress-tab	A-CHA-CHAM- 170523/62
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via a crafted payload to the personal notes function. <b>CVE ID : CVE-2023-</b> <b>31807</b>	https://supp ort.chamilo.o rg/projects/ chamilo- 18/wiki/Sec urity_issues #Issue-101- 2023-04-11- Low-impact- Low-risk- XSS-in- personal- notes-and- teacher- notes	A-CHA-CHAM- 170523/63
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the system annnouncements parameter. <b>CVE ID : CVE-2023-</b> <b>31799</b>	https://supp ort.chamilo.o rg/projects/ chamilo- 18/wiki/Sec urity_issues #Issue-99- 2023-04-11- Low-impact- Low-risk- XSS-in- system-	A-CHA-CHAM- 170523/64

0-1

1-2

2-33-44-5Page 41 of 1106

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				announceme nts	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the resource sequencing parameters. <b>CVE ID : CVE-2023-</b> <b>31803</b>	https://supp ort.chamilo.o rg/projects/ chamilo- 18/wiki/Sec urity_issues #Issue-100- 2023-04-11- Low-impact- Low-risk- XSS-in- resources- sequencing	A-CHA-CHAM- 170523/65
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local authenticated attacker to execute arbitrary code via the homepage function. <b>CVE ID : CVE-2023-</b> <b>31805</b>	https://supp ort.chamilo.o rg/projects/ chamilo- 18/wiki/Sec urity_issues #Issue-98- 2023-04-11- Low-impact- Low-risk- XSS-in- homepage- edition	A-CHA-CHAM- 170523/66
Vendor: chu	ırchcrm				
Product: ch	urchcrm				
	sion(s): 4.5.4				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	04-May-2023	9.8	ChurchCRM 4.5.4 endpoint /EditEventTypes.php is vulnerable to Blind SQL Injection (Time- based) via the EN_tyid POST parameter. CVE ID : CVE-2023- 29842	N/A	A-CHU-CHUR- 170523/67

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: clio	)	<u>.</u>			
Product: cli	o_grow				
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Themis Solutions, Inc. Clio Grow plugin <= 1.0.0 versions. <b>CVE ID : CVE-2023-</b> <b>22683</b>	N/A	A-CLI-CLIO- 170523/68
Vendor: clo	ud_manager_pro	oject			
Product: clo	ud_manager				
Affected Ver	sion(s): * Up to (i	ncluding)	1.0		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	6.1	The Cloud Manager WordPress plugin through 1.0 does not sanitise and escape the query param ricerca before outputting it in an admin panel, allowing unauthenticated attackers to trick a logged in admin to trigger a XSS payload by clicking a link. <b>CVE ID : CVE-2023-</b> <b>0421</b>	N/A	A-CLO-CLOU- 170523/69
Vendor: cltp	_				
Product: clt		1 1	( )		
	sion(s): * Up to (i	ncluding)			1
Unrestricte d Upload of File with Dangerous Type	04-May-2023	9.8	CLTPHP <=6.0 is vulnerable to Unrestricted Upload of File with Dangerous Type via	N/A	A-CLT-CLTP- 170523/70

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 <b>43</b> of	1106					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application/admin/c ontroller/Template.p hp:update.		
			CVE ID : CVE-2023- 30264		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-May-2023	9.8	CLTPHP <=6.0 is vulnerable to Improper Input Validation. CVE ID : CVE-2023- 30268	N/A	A-CLT-CLTP- 170523/71
Vendor: cm	s_press_project				
Product: cm	is_press				
Affected Ver	sion(s): * Up to (i	ncluding)	0.2.3		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site	08-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Michael Pretty (prettyboymp) CMS Press plugin <= 0.2.3 versions. <b>CVE ID : CVE-2023-</b>	N/A	A-CMS-CMS 170523/72
Scripting')			25452		
Vendor: cod	lestag				
Product: sta	gtools				
Affected Ver	sion(s): * Up to (e	excluding)	2.3.7		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	5.4	The StagTools WordPress plugin before 2.3.7 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which	N/A	A-COD-STAG- 170523/73

0-1

1-2

3-4 4-5 2-3 Page 44 of 1106

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.		
			CVE ID : CVE-2023- 0891		
Vendor: con	itrolid				
Product: rhi	id				
Affected Vers	sion(s): 23.3.19.0	)			
Direct Request ('Forced Browsing')	04-May-2023	9.8	A vulnerability classified as critical has been found in Control iD RHiD 23.3.19.0. This affects an unknown part of the file /v2/#/. The manipulation leads to direct request. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB- 228015. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. <b>CVE ID : CVE-2023- 2524</b>	N/A	A-CON-RHID- 170523/74
Vendor: con		<b>1 1</b>			
	nvertbox_auto_e		10.20		
Improper Neutralizat ion of Input	<mark>sion(s): * Up to (6</mark> 09-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in	N/A	A-CON-CONV- 170523/75
CVSS Scoring S	Scale 0-1 2	L-2 2-3	<b>3-4 4-5 5-6</b> Page <b>45</b> of <b>1106</b>	6-7 7-	8 8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			ConvertBox ConvertBox Auto Embed WordPress plugin <= 1.0.19 versions.		
			CVE ID : CVE-2023- 23664		
Vendor: cre	ativethemes			L	l
Product: blo	ocksy_companio	n			
Affected Ver	sion(s): * Up to (e	excluding)	1.8.82		
Authorizati on Bypass Through User- Controlled Key	02-May-2023	4.3	The Blocksy Companion WordPress plugin before 1.8.82 does not ensure that posts to be accessed via a shortcode are already public and can be viewed, allowing any authenticated users, such as subscriber to access draft posts for example <b>CVE ID : CVE-2023-</b>	N/A	A-CRE-BLOC- 170523/76
			1911		
Vendor: crn					
Product: cri		مان بال ۲۰		( )	
Allected ver	sion(s): From (in		.4.0 Up to (including) 4	.0.0	
Unrestricte d Upload of File with Dangerous Type	08-May-2023	9.8	CRMEB v4.4 to v4.6 was discovered to contain an arbitrary file upload vulnerability via the component \attachment\System AttachmentServices. php. CVE ID : CVE-2023- 30185	N/A	A-CRM-CRME- 170523/77

0-1

1-2

3-4 4-5 2-3 Page 46 of 1106

6-7

5-6

8-9

9-10

m_login_page m_login_page n(s): * Up to (i 4-May-2023 m_more_link_ m_more_link n(s): * Up to (i	4.8 complete	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Denzel Chia   Phire Design Custom Login Page plugin <= 2.0 versions. CVE ID : CVE-2023- 26012 e_project	N/A	A-CUS-CUST- 170523/78
n(s): * Up to (i 4-May-2023 m_more_link_ m_more_link n(s): * Up to (i	4.8 complete	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Denzel Chia   Phire Design Custom Login Page plugin <= 2.0 versions. CVE ID : CVE-2023- 26012 e_project te 1.4.1 Auth. (admin+) Stored Cross-Site Scripting (XSS)	N/A	
4-May-2023 m_more_link_ m_more_link_ n(s): * Up to (i	4.8 .complete _complete	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Denzel Chia   Phire Design Custom Login Page plugin <= 2.0 versions. CVE ID : CVE-2023- 26012 e_project te 1.4.1 Auth. (admin+) Stored Cross-Site Scripting (XSS)	N/A	
m_more_link_ m_more_link n(s): * Up to (i	_complete _complet	Stored Cross-Site Scripting (XSS) vulnerability in Denzel Chia   Phire Design Custom Login Page plugin <= 2.0 versions. CVE ID : CVE-2023- 26012 e_project e 1.4.1 Auth. (admin+) Stored Cross-Site Scripting (XSS)	N/A	
m_more_link n(s): * Up to (i	_complet	26012 e_project e 1.4.1 Auth. (admin+) Stored Cross-Site Scripting (XSS)		
m_more_link n(s): * Up to (i	_complet	e 1.4.1 Auth. (admin+) Stored Cross-Site Scripting (XSS)		
n(s): * Up to (i	-	1.4.1 Auth. (admin+) Stored Cross-Site Scripting (XSS)		
	ncluding)	Auth. (admin+) Stored Cross-Site Scripting (XSS)		
0-Mav-2023		Stored Cross-Site Scripting (XSS)		
	4.8	Florin Arjocu Custom More Link Complete plugin <= 1.4.1 versions. <b>CVE ID : CVE-2023-</b>	N/A	A-CUS-CUST- 170523/79
		23788		
		1010101		
n(s): * Up to (e	excluding	1.0.10.1646		1
8-May-2023	6.1	Cybonet PineApp Mail Secure A reflected cross-site scripting (XSS) vulnerability was identified in the product, using an unspecified endpoint.	N/A	A-CYB-PINE- 170523/80
r	n(s): * Up to (e	pp_mail_secure n(s): * Up to (excluding)	et pp_mail_secure h(s): * Up to (excluding) 1.0.10.1646 Cybonet PineApp Mail Secure A reflected cross-site scripting (XSS) vulnerability was identified in the product, using an unspecified	et pp_mail_secure h(s): * Up to (excluding) 1.0.10.1646 Cybonet PineApp Mail Secure A reflected cross-site scripting (XSS) vulnerability was identified in the product, using an unspecified

Page **47** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 31183		
Vendor: Del	<u> </u>				
	enware_comma	nd_cente	r		
	_ sion(s): * Up to (e				
Improper Access Control	03-May-2023	7.8	Alienware Command Center Application, versions 5.5.43.0 and prior, contain an improper access control vulnerability. A local malicious user could potentially exploit this vulnerability during installation or update process leading to privilege escalation. <b>CVE ID : CVE-2023- 28070</b>	https://ww w.dell.com/s upport/kbdo c/en- us/0002122 77/dsa- 2023-135	A-DEL-ALIE- 170523/81
	mmand_\ _mon		10.0		
Affected Ver- Incorrect Permission Assignmen t for	<mark>sion(s): * Up to (</mark> i 05-May-2023	ncluding) 7.8	10.9 Dell Command Monitor, versions 10.9 and prior, contains an	https://ww w.dell.com/s upport/kbdo c/en- us/0002122	A-DEL-COMM- 170523/82
CVSS Scoring S	Scale 0-1 C	L-2 2-3	<b>3-4 4-5 5-6</b> Page <b>48</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			improper folder permission vulnerability. A local authenticated malicious user can potentially exploit this vulnerability leading to privilege escalation by writing to a protected directory when Dell Command Monitor is installed to a non- default path <b>CVE ID : CVE-2023- 28068</b>	26/dsa- 2023-133	
Product: ela	astic_cloud_stora	age			
Affected Ver	sion(s): * Up to (	excluding)	3.8.0.2		
Improper Verificatio n of Cryptograp hic Signature	04-May-2023	7.5	DELL ECS prior to 3.8.0.2 contains an improper verification of cryptographic signature vulnerability. A network attacker with an ability to intercept the request could potentially exploit this vulnerability to modify the body data of the request.	https://ww w.dell.com/s upport/kbdo c/en- us/0002129 70/dsa- 2023-109- dell-ecs- security- update-for- multiple- vulnerabiliti es	A-DEL-ELAS- 170523/83
			CVE ID : CVE-2023- 25934		

0-1

1-2

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Vendor: dev	olutions	I		I	L				
Product: de	Product: devolutions_server								
Affected Ver	sion(s): * Up to (e	excluding)	2023.1.3.0						
N/A	02-May-2023	4.9	Improper access control in Subscriptions Folder path filter in Devolutions Server 2023.1.1 and earlier allows attackers with administrator privileges to retrieve usage information on folders in user vaults via a specific folder name. <b>CVE ID : CVE-2023-</b>	https://devo lutions.net/s ecurity/advi sories/DEVO -2023-0013/	A-DEV-DEVO- 170523/84				
Vendor: dig	italdruid		2445						
Product: ho	tel_druid								
Affected Ver	sion(s): 3.0.4								
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	5.4	A Stored Cross Site Scripting (XSS) vulnerability exists in multiple pages of Hotel Druid version 3.0.4, which allows arbitrary execution of commands. The vulnerable fields are Surname, Name, and Nickname in the Document function. <b>CVE ID : CVE-2023-</b>	N/A	A-DIG-HOTE- 170523/85				
			29839						
	qus_conditional		oject						
	squs_conditiona		11.0.6						
Affected Ver	sion(s): * Up to (i	ncluding)	11.0.6						

0-1

1-2

2-3

**3-4 4-5** Page **50** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Joel James Disqus Conditional Load plugin <= 11.0.6 versions. CVE ID : CVE-2023- 23732	N/A	A-DIS-DISQ- 170523/86
Vendor: Dja	ingoproject				
Product: dja	ango				
Affected Ver	sion(s): 4.2				
Improper Input Validation	07-May-2023	9.8	In Django 3.2 before 3.2.19, 4.x before 4.1.9, and 4.2 before 4.2.1, it was possible to bypass validation when using one form field to upload multiple files. This multiple upload has never been supported by forms.FileField or forms.ImageField (only the last uploaded file was validated). However, Django's "Uploading multiple files" documentation suggested otherwise. <b>CVE ID : CVE-2023- 31047</b>	https://ww w.djangoproj ect.com/web log/2023/m ay/03/secur ity-releases/, https://docs. djangoprojec t.com/en/4. 2/releases/s ecurity/	A-DJA-DJAN- 170523/87
Affected Ver	sion(s): From (in	cluding) 3	.2 Up to (excluding) 3.2	.19	
Improper Input Validation	07-May-2023	9.8	In Django 3.2 before 3.2.19, 4.x before 4.1.9, and 4.2 before 4.2.1, it was possible to bypass validation	https://ww w.djangoproj ect.com/web log/2023/m ay/03/secur	A-DJA-DJAN- 170523/88

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			when using one form field to upload multiple files. This multiple upload has never been supported by forms.FileField or forms.ImageField (only the last uploaded file was validated). However, Django's "Uploading multiple files" documentation suggested otherwise.	ity-releases/, https://docs. djangoprojec t.com/en/4. 2/releases/s ecurity/				
			CVE ID : CVE-2023- 31047					
Affected Ver	<mark>sion(s): From (in</mark>	cluding) 4	.0 Up to (excluding) 4.1	.9	I			
Improper Input Validation	07-May-2023	9.8	In Django 3.2 before 3.2.19, 4.x before 4.1.9, and 4.2 before 4.2.1, it was possible to bypass validation when using one form field to upload multiple files. This multiple upload has never been supported by forms.FileField or forms.ImageField (only the last uploaded file was validated). However, Django's "Uploading multiple files" documentation suggested otherwise. <b>CVE ID : CVE-2023- 31047</b>	https://ww w.djangoproj ect.com/web log/2023/m ay/03/secur ity-releases/, https://docs. djangoprojec t.com/en/4. 2/releases/s ecurity/	A-DJA-DJAN- 170523/89			
Vendor: dmtf								
Product: libspdm								
CVSS Scoring	Scale 0-1	1-2 2-3	3-4 4-5 5-6	6 6-7 7-8	<u> </u>			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Ver	Affected Version(s): * Up to (excluding) 2.3.2								
Affected Vers	sion(s): * Up to (e	excluding) 8.8	2.3.2 libspdm is a sample implementation that follows the DMTF SPDM specifications. A vulnerability has been identified in SPDM session establishment in libspdm prior to version 2.3.1. If a device supports both DHE session and PSK session with mutual authentication, the attacker may be able to establish the session with `KEY_EXCHANGE` and `PSK_FINISH` to bypass the mutual authentication. This is most likely to happen when the Requester begins a session using one method (DHE, for example) and then uses the other method's finish (PSK_FINISH in this example) to establish the session. The session hashes would be expected to fail in this case, but the condition was not detected.	https://githu b.com/DMTF /libspdm/se curity/advis ories/GHSA- qw76-4v8p- xq9f, https://githu b.com/DMTF /libspdm/pu ll/2007, https://githu b.com/DMTF /libspdm/pu ll/2006	A-DMT-LIBS- 170523/90				
			supports						

0-1

1-2

2-33-44-5Page 53 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`KEY_EX_CAP=1 and `PSK_CAP=10b` at same time with mutual authentication requirement. The SPDM requester is not impacted. The SPDM responder is not impacted if `KEY_EX_CAP=0` or `PSK_CAP=0` or `PSK_CAP=0`b`. The SPDM responder is not impacted if mutual authentication is not required. Ilibspdm 1.0, 2.0, 2.1, 2.2, 2.3 are all impacted. Older branches are not maintained, but users of the 2.3 branch may receive a patch in version 2.3.2. The SPDM specification (DSP0274) does not contain this vulnerability.		
			31127		
Vendor: dou					
Product: do					
Affected Vers	sion(s): 1.7				
Improper Neutralizat ion of Input During	03-May-2023	4.8	A stored cross-site scripting (XSS) vulnerability in DouPHP v1.7 allows attackers to execute	N/A	A-DOU-DOUP- 170523/91
CVSS Scoring S	icale 0-1	L-2 2-3	<b>3</b> 3-4 4-5 5-6	6-7 7	<sup>7</sup> -8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			arbitrary web scripts or HTML via a crafted payload injected into the unique_id parameter in /admin/article.php. <b>CVE ID : CVE-2023-</b> <b>30205</b>		
Vendor: dre	eamer_cms_proj	ect	L		1
Product: dr	eamer_cms				
Affected Ver	sion(s): * Up to (i	ncluding)	4.1.3		
Inefficient Algorithmi c Complexity	02-May-2023	7.5	A vulnerability was found in Dreamer CMS up to 4.1.3. It has been declared as problematic. This vulnerability affects the function updatePwd of the file UserController.java of the component Password Hash Calculation. The manipulation leads to inefficient algorithmic complexity. The attack can be initiated remotely. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB- 227860. <b>CVE ID : CVE-2023-</b> 2473	N/A	A-DRE-DREA- 170523/92
Vendor: e-o					
Product: e-o Affected Ver					
0.462.0					
CVSS Scoring S	Scale 0-1 :	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>55</b> of <b>1106</b>	6-7 7-8	3 8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricte d Upload of File with Dangerous Type	04-May-2023	9.8	A vulnerability was found in Weaver E- Office 9.5. It has been rated as critical. Affected by this issue is some unknown functionality of the file App/Ajax/ajax.php?a ction=mobile_upload _save. The manipulation of the argument upload_quwan leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB- 228014 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. <b>CVE ID : CVE-2023- 2523</b>	N/A	A-E-O-E-OF- 170523/93
Vendor: eas Product: eas	<u> </u>				
Affected Ver					
Authorizati on Bypass Through User- Controlled Key	08-May-2023	9.8	EasyTor Applications – Authorization Bypass - EasyTor Applications may allow authorization	N/A	A-EAS-EASY- 170523/94

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass via unspecified method. <b>CVE ID : CVE-2023-</b>		
Vendor: eas	y_event_calenda	ar proiec	31182 t		
	sy_event_calend		•		
	sion(s): * Up to (i		1.0		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in CoreFortress Easy Event calendar plugin <= 1.0 versions. <b>CVE ID : CVE-2023- 28169</b>	N/A	A-EAS-EASY- 170523/95
Vendor: ech	_				
Product: iud					
Affected Ver	sion(s): From (in	cluding) 5	5.15.0 Up to (excluding)	6.27.6	
Use of Hard- coded Credentials	02-May-2023	9.8	European Chemicals Agency IUCLID 6.x before 6.27.6 allows authentication bypass because a weak hard-coded secret is used for JWT signing. The affected versions are 5.15.0 through 6.27.5. <b>CVE ID : CVE-2023-</b> <b>26089</b>	https://iucli d6.echa.euro pa.eu/docu ments/1387 205/180953 0/note_v6.2 7.6.pdf/7654 5a65-e6be- 6486-280a- 7d7c3d2ad4 55?t=16775 77170669	A-ECH-IUCL- 170523/96

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-May-2023	8.8	European Chemicals Agency IUCLID before 6.27.6 allows remote authenticated users to execute arbitrary code via Server Side Template Injection (SSTI) with a crafted template file. The attacker must have template manager permission. <b>CVE ID : CVE-2023-</b> <b>26546</b>	https://iucli d6.echa.euro pa.eu/docu ments/1387 205/180953 0/note_v6.2 7.6.pdf/7654 5a65-e6be- 6486-280a- 7d7c3d2ad4 55?t=16775 77170669	A-ECH-IUCL- 170523/97
Vendor: effe	ectindex				
Product: tri					
Affected Ver	sion(s): * Up to (	excluding)		1	
Improper Authentica tion	08-May-2023	9.1	<pre>`effectindex/triprepo rter` is a community- powered, universal platform for submitting and analyzing trip reports. Prior to commit bd80ba833b9023d3 9ca22e29874296c87 29dd53b, any user with an account on an instance of `effectindex/triprepo rter`, e.g. `subjective.report`, may be affected by an improper password verification vulnerability. The vulnerability allows any user with a password matching</pre>	https://githu b.com/effect index/tripre porter/secur ity/advisorie s/GHSA- 356r-rwp8- h6m6, https://githu b.com/effect index/tripre porter/com mit/bd80ba 833b9023d3 9ca22e2987 4296c8729d d53b	A-EFF-TRIP- 170523/98

0-1

1-2

2-33-44-5Page 58 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the password requirements to log in as any user. This allows access to accounts / data loss of the user. This issue is patched in commit bd80ba833b9023d3 9ca22e29874296c87 29dd53b. No action necessary for users of `subjective.report`, and anyone running their own instance should update to this commit or newer as soon as possible. As a workaround, someone running their own instance may apply the patch manually. <b>CVE ID : CVE-2023- 31123</b>		
Vendor: ejs					
Product: ejs					
Affected Versi	ion(s): 3.1.9				
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection' )	04-May-2023	9.8	ejs v3.1.9 is vulnerable to server- side template injection. If the ejs file is controllable, template injection can be implemented through the configuration settings of the closeDelimiter parameter. <b>CVE ID : CVE-2023- 29827</b>	https://githu b.com/mde/ ejs/issues/7 20	A-EJS-EJS- 170523/99
CVSS Scoring Sc	ale 0-1 1	2 2-3	<b>3-4 4-5 5-6</b> Page <b>59</b> of <b>1106</b>	6-7 7-8	3 8-9 <mark>9-10</mark>

Page **59** of **1106** 

Vendor: Elastic         Product: filebeat         Affected Version(s): * Up to (including) 7.17.9         Insertion of Sensitive Informatio n into Log         File         Insertion of Sensitive Informatio of Sensitive Informatio of Sensitive Informatio n into Log         Prile         Insertion of Sensitive Informatio Into Log       A.ELA-FILE-         Product: kibana       8.8       Kibana version 8.7.0 contains an arbitrary code execution flav. An attacker with All privileges to the Uptime/Synthetics feature could send a.7.0, thtps://disc uss.elastic.co/ community/ security/, https://disc uss.elastic.co/ security/, Security/, https://security/, Security/, Security/, Security/, Security/, Security/, Security/, Se	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 7.17.9Insertion of Sensitive Informatio n into Log File04-May-20233.3Filebeat versions through 7.17.9 and 8.6.2 have a flaw in httpision input that allows the http request Authorization or Proxy-Authorization header contents to be leaked in the logs when debug logging is enabled. CVE ID : CVE-2023- 31413https://ww welastic.co/ roty-Authorization roty-Authorization request stack 8-7-0- 7.17-10- security- updates/332A-ELA-FILE- 170523/100Affected Version(s): 8.6.2Filebeat versions through 7.17.9 and 8.6.2 have a flaw in https://ww welastic.co/ community/ security- updates/332https://ww welastic.co/ community/ security- updates/332Affected Version(s): 8.6.2Filebeat versions through 7.17.9 and 8.6.2 have a flaw in https://ww welastic.co/ community/ security- updates/332https://ww welastic.co/ community/ security/ https://disc usselastic.co //elastic- stack 8-7.0- 7.17.10- security- updates/332A-ELA-FILE- 170523/101Insertion of Sensitive Informatio File04-May-20233.3Filebeat versions through 7.17.9 and 8.6.2 have a flaw in https://as usselastic.co/ community/ security- updates/332A-ELA-FILE- 170523/101Product: kibamaA-ELA-FILE- A-ELA-FILE- 170523/101A-ELA-FILE- 170523/101Insertion of Code (Code (Code (Code) (Code (Code) (Code) (Code) (Code) (Code) (Code)B.8Kibana version 8.7.0 Contains an arbitrary code execution flaw. An attacker with All privileges to the Upti	Vendor: Ela	stic	I			
Insertion of Sensitive Information n into Log04-May-20233.3Filebeat versions through 7.17.9 and 8.6.2 have a flaw in httpision input that allows the http request Authorization or Proxy-Authorization header contents to be leaked in the logs when debug logging is enabled. CVE ID : CVE-2023- 31413https://ww we.lastic.co /t/elastic sacurity. https://disc uuss.elastic.co /t/elastic sacurity. https://disc uuss.elastic.co /t/elastic sacurity. https://ww we.lastic.co/ community/ security.A-ELA-FILE- 170523/100Affected Version(s): 8.6.2Filebeat versions through 7.17.9 and 8.6.2 have a flaw in https:/oisc uuss.elastic.co/ community/ security. https://disc uuss.elastic.co/ community/ security. https://disc uuss.elastic.co/ /community/ security.A-ELA-FILE- 170523/100Insertion of Sensitive Informatio rinto Log File04-May-20233.3Filebeat versions through 7.17.9 and 8.6.2 have a flaw in https://oisc uuss.elastic.co/ /community/ security. https://disc uuss.elastic.co/ //elastic- sack-8-7-0- 7.17-10- security. pdates/332A-ELA-FILE- 170523/101Insertion of Sensitive File04-May-20238.8Kibana version 8.7.0 contains an arbitrary code execution flaw. An attacker with All privileges to the Uptime/Synthetics fature could sead allow in privileges to the Uptime/Synthetics fature could sead allow in the allow sead allow in the allow sead allow is enabled. CVE ID : CVE-2023- 327https://ww we.lastic.co/ community/ security. https://disc uuss.elastic.co/ community/ security. https://disc <td>Product: file</td> <td>ebeat</td> <td></td> <td></td> <td></td> <td></td>	Product: file	ebeat				
Insertion of Sensitive Information n into Log 	Affected Vers	sion(s): * Up to (i	ncluding)	7.17.9		
Insertion of Sensitive Informatio n into Log File04-May-20233.3Filebeat versions through 7.17.9 and 8.6.2 have a flaw in https://isc allows the http request Authorization or Proxy-Authorization header contents to be leaked in the logs yrith alta security- header contents to be leaked in the logs yrith alta security- updates/332A-ELA-FILE- 170523/101Product: kibaraKibana version 8.7.0 control of Generation of Code ('Code lnjection')Kibana version 8.7.0 code execution flaw. An attacker with All privileges to the privileges to the privileges to the https://disc uss.elastic.co/ code execution flaw.A-ELA-KIBA- fity-integrity- A-ELA-KIBA- fity-integrity- alty-integrity- security- updates/332Improper Control of Generation of Code ('Code lnjection')04-May-20238.8Kibana version 8.7.0 privileges to the privileges to the privileges to the https://kibianahttps://ww https://kibianaImproper Control of Generation of Code ('Code lnjection')04-May-20238.8Kibana version 8.7.0 privileges to the privileges to the https://kibianahttps://ww https://kibianaImproper (Code lnjection')04-May-20238.8Kibana version 8.7.0 privileges to the privileges to the https://kibianahttps://accor/ privileges to the https://kibianaA-ELA-KIBA- privileges to the https://kibiana	of Sensitive Informatio n into Log	04-May-2023	3.3	through 7.17.9 and 8.6.2 have a flaw in httpjson input that allows the http request Authorization or Proxy-Authorization header contents to be leaked in the logs when debug logging is enabled. <b>CVE ID : CVE-2023-</b>	w.elastic.co/ community/ security/, https://disc uss.elastic.co /t/elastic- stack-8-7-0- 7-17-10- security- updates/332	
Insertion of Sensitive Informatio n into Log File04-May-2023and same and Samethrough 7.17.9 and 8.6.2 have a flaw in httpsion input that allows the http request Authorization or Proxy-Authorization Proxy-Authorization be leaked in the logs when debug logging is enabled. UPA the security- updates/332https://ww w.elastic.co/ /t/elastic- stack-8-7-0- 7-17-10- security- updates/332A-ELA-FILE- 170523/101Product: kibra CVE ID : CVE-2023- 31413Zere and and contains an arbitrary conde a community/ welastic.co/ code execution flaw. An attacker with All privileges to the uptime/Synthetics (code liget in selastic.co) /t/kibana-8-https://ww w.elastic.co/ the security- updates/332A-ELA-FILE- 170523/101Improper Control of Generation of Code ('Code Injection')04-May-20238.8Kibana version 8.7.0 An attacker with All privileges to the uptime/Synthetics (security/, https://dischttps://ww w.elastic.co/ community/ security/, https://disc	Affected Vers	sion(s): 8.6.2			L	
Affected Version(s): 8.7.0Improper Control of Generation of Code ('Code Injection')04-May-2023Kibana version 8.7.0 contains an arbitrary contains an arbitrary code execution flaw. An attacker with All privileges to the Uptime/Synthetics feature could send ahttps://ww w.elastic.co/ community/ https://disc uss.elastic.co	of Sensitive Informatio n into Log	04-May-2023	3.3	through 7.17.9 and 8.6.2 have a flaw in httpjson input that allows the http request Authorization or Proxy-Authorization header contents to be leaked in the logs when debug logging is enabled. <b>CVE ID : CVE-2023-</b>	w.elastic.co/ community/ security/, https://disc uss.elastic.co /t/elastic- stack-8-7-0- 7-17-10- security- updates/332	
Improper Control of Generation of Code ('Code Injection')04-May-20238.8Kibana version 8.7.0 contains an arbitrary contains an arbitrary code execution flaw. An attacker with All privileges to the Uptime/Synthetics feature could send ahttps://ww w.elastic.co/ A-ELA-KIBA- 170523/102Improper ('Code Injection')04-May-20238.88.8Kibana version 8.7.0 contains an arbitrary code execution flaw. Mattacker with All privileges to the Uptime/Synthetics feature could send ahttps://disc typical https://discA-ELA-KIBA- 170523/102	Product: kit	oana		<u> </u>		
Improper Control of Generation of Code ('Code Injection')04-May-20238.8contains an arbitrary code execution flaw. An attacker with All privileges to the Uptime/Synthetics feature could send aw.elastic.co/ community/ https://disc uss.elastic.co /t/kibana-8-A-ELA-KIBA- 170523/102	Affected Vers	sion(s): 8.7.0				
	Control of Generation of Code ('Code	04-May-2023	8.8	contains an arbitrary code execution flaw. An attacker with All privileges to the Uptime/Synthetics	w.elastic.co/ community/ security/, https://disc uss.elastic.co	
UVSS Scoring Scale U-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1	CVSS Scoring S	icale 0-1	L-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			
			request that will attempt to execute JavaScript code. This could lead to the attacker executing arbitrary commands on the host system with permissions of the Kibana process. <b>CVE ID : CVE-2023-</b> <b>31415</b>	7-1-security- updates/332 330				
Affected Ver	sion(s): From (in	cluding) 8	.0.0 Up to (including) 8.	7.0				
Improper Control of Generation of Code ('Code Injection')	04-May-2023	8.8	Kibana versions 8.0.0 through 8.7.0 contain an arbitrary code execution flaw. An attacker with write access to Kibana yaml or env configuration could add a specific payload that will attempt to execute JavaScript code. This could lead to the attacker executing arbitrary commands on the host system with permissions of the Kibana process. <b>CVE ID : CVE-2023-</b> <b>31414</b>	https://ww w.elastic.co/ community/ security/, https://disc uss.elastic.co /t/kibana-8- 7-1-security- updates/332 330	A-ELA-KIBA- 170523/103			
Vendor: em	qx							
Product: nanomq								
Affected Ver	sion(s): 0.15.0							
Out-of- bounds Write	04-May-2023	7.5	In NanoMQ v0.15.0- 0, Heap overflow occurs in read_byte function of mqtt_code.c.	N/A	A-EMQ-NANO- 170523/104			

CVSS Scoring	Scale	
--------------	-------	--

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			CVE ID : CVE-2023- 29994				
Out-of- bounds Write	04-May-2023	7.5	In NanoMQ v0.15.0- 0, a Heap overflow occurs in copyn_utf8_str function of mqtt_parser.c CVE ID : CVE-2023- 29995	N/A	A-EMQ-NANO- 170523/105		
NULL Pointer Dereferenc e	04-May-2023	7.5	In NanoMQ v0.15.0- 0, segment fault with Null Pointer Dereference occurs in the process of decoding subinfo_decode and unsubinfo_decode. <b>CVE ID : CVE-2023- 29996</b>	N/A	A-EMQ-NANO- 170523/106		
Vendor: ena	able\/disable_a	uto_login_	when_register_projec	t			
	able\/disable_a	_					
Affected Ver	sion(s): * Up to (i	ncluding)	1.1.0				
Cross-Site Request Forgery (CSRF)	08-May-2023	6.5	The Enable/Disable Auto Login when Register WordPress plugin through 1.1.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	N/A	A-ENA-ENAB- 170523/107		
Vendor: Ena	alean		0522				
Product: tul							
	-	cluding) 1	4.7.99.76 Up to (exclud	ing) 14.7.99.14	3		
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10							
evos scoring :		<u> </u>	Page <b>62</b> of <b>1106</b>				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	5.4	Tuleap Open ALM is a Libre and Open Source tool for end to end traceability of application and system developments. The title of an artifact is not properly escaped in the tooltip. A malicious user with the capability to create an artifact or to edit a field title could force victim to execute uncontrolled code. This issue has been patched in version 14.7.99.143. <b>CVE ID : CVE-2023- 30619</b>	https://githu b.com/Enale an/tuleap/se curity/advis ories/GHSA- 7fm3-cr3g- 5922, https://tulea p.net/plugin s/git/tuleap/stab le?a=commit &h=fdc93a7 36cbccad05 de16ff0cc7cc 3ef18dc93df, https://tulea p.net/plugin s/tracker/?a id=31586	A-ENA-TULE- 170523/108				
Vendor: enh	nanced_wp_cont	act_form_	project	I	L				
Product: en	hanced_wp_con	tact_form	L						
Affected Ver	sion(s): * Up to (i	ncluding)	2.2.3						
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Joost de Valk Enhanced WP Contact Form plugin <= 2.2.3 versions. <b>CVE ID : CVE-2023- 23812</b>	N/A	A-ENH-ENHA- 170523/109				
Vendor: Esr	'i								
Product: po	Product: portal_for_arcgis								
Affected Ver	sion(s): 10.7.1								
Improper Neutralizat	09-May-2023	6.1	There is a reflected XSS vulnerability in	https://ww w.esri.com/a	A-ESR-PORT- 170523/110				
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 63 of 1106								

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. <b>CVE ID : CVE-2023- 25830</b>	rcgis- blog/produc ts/trust- arcgis/admi nistration/p ortal-for- arcgis- security- 2023- update-1- patch-is- now- available/	
Affected Ver	sion(s): 10.8.1				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. <b>CVE ID : CVE-2023- 25830</b>	https://ww w.esri.com/a rcgis- blog/produc ts/trust- arcgis/admi nistration/p ortal-for- arcgis- security- 2023- update-1- patch-is- now- available/	A-ESR-PORT- 170523/111
Affected Ver	sion(s): 10.9.1		<u> </u>		
URL Redirectio n to Untrusted Site ('Open Redirect')	09-May-2023	6.1	There is an unvalidated redirect vulnerability in Esri Portal for ArcGIS 11.0 and 10.9.1 that may allow a remote, unauthenticated attacker to craft a	https://ww w.esri.com/a rcgis- blog/produc ts/trust- arcgis/admi nistration/p ortal-for-	A-ESR-PORT- 170523/112

0-1

1-2

5-6

6-7

7-8

8-9

Weakness P	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			URL that could redirect a victim to an arbitrary website, simplifying phishing attacks. CVE ID : CVE-2023- 25829	arcgis- security- 2023- update-1- patch-is- now- available/	
Improper Neutralizat ion of Input During 09- Web Page Generation ('Cross-site Scripting')	-May-2023	6.1	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. <b>CVE ID : CVE-2023- 25830</b>	https://ww w.esri.com/a rcgis- blog/produc ts/trust- arcgis/admi nistration/p ortal-for- arcgis- security- 2023- update-1- patch-is- now- available/	A-ESR-PORT- 170523/113
Affected Version	ı(s): 11.0				
URL Redirectio n to Untrusted Site ('Open Redirect')	-May-2023	6.1	There is an unvalidated redirect vulnerability in Esri Portal for ArcGIS 11.0 and 10.9.1 that may allow a remote, unauthenticated attacker to craft a URL that could redirect a victim to an arbitrary website, simplifying phishing attacks.	https://ww w.esri.com/a rcgis- blog/produc ts/trust- arcgis/admi nistration/p ortal-for- arcgis- security- 2023- update-1- patch-is-	A-ESR-PORT- 170523/114
			CVE ID : CVE-2023- 25829	now- available/	

0-1

1-2

2-3

**3-4 4-5** Page **65** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ev	asys	I		L	
Affected Ver	sion(s): 8.2				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	8.8	A SQL injection issue in Logbuch in evasys before 8.2 Build 2286 and 9.x before 9.0 Build 2401 allows authenticated attackers to execute SQL statements via the welche parameter. <b>CVE ID : CVE-2023-</b> <b>31433</b>	N/A	A-EVA-EVAS- 170523/115
Incorrect Authorizati on	02-May-2023	8.1	Multiple components (such as Onlinetemplate- Verwaltung, Liste aller Teilbereiche, Umfragen anzeigen, and questionnaire previews) in evasys before 8.2 Build 2286 and 9.x before 9.0 Build 2401 allow authenticated attackers to read and write to unauthorized data by accessing functions directly. <b>CVE ID : CVE-2023-</b> <b>31435</b>	N/A	A-EVA-EVAS- 170523/116
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	5.4	The parameters nutzer_titel, nutzer_vn, and nutzer_nn in the user profile, and langID and ONLINEID in direct links, in evasys before 8.2 Build 2286 and 9.x before	N/A	A-EVA-EVAS- 170523/117

0-1

1-2

2-3

**3-4 4-5** Page **66** of **1106**  5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.0 Build 2401 do not validate input, which allows authenticated attackers to inject HTML Code and XSS payloads in multiple locations.		
			CVE ID : CVE-2023- 31434		
Affected Ver	sion(s): 9.0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	8.8	A SQL injection issue in Logbuch in evasys before 8.2 Build 2286 and 9.x before 9.0 Build 2401 allows authenticated attackers to execute SQL statements via the welche parameter. <b>CVE ID : CVE-2023-</b> <b>31433</b>	N/A	A-EVA-EVAS- 170523/118
Incorrect Authorizati on	02-May-2023	8.1	Multiple components (such as Onlinetemplate- Verwaltung, Liste aller Teilbereiche, Umfragen anzeigen, and questionnaire previews) in evasys before 8.2 Build 2286 and 9.x before 9.0 Build 2401 allow authenticated attackers to read and write to unauthorized data by accessing functions directly. <b>CVE ID : CVE-2023- 31435</b>	N/A	A-EVA-EVAS- 170523/119

0-1

1-2

2-33-44-5Page 67 of 1106

5-6

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	5.4	The parameters nutzer_titel, nutzer_vn, and nutzer_nn in the user profile, and langID and ONLINEID in direct links, in evasys before 8.2 Build 2286 and 9.x before 9.0 Build 2401 do not validate input, which allows authenticated attackers to inject HTML Code and XSS payloads in multiple locations.	N/A	A-EVA-EVAS- 170523/120		
			CVE ID : CVE-2023- 31434				
Vendor: exq	luisite_paypal_d	onation_j	project				
	quisite_paypal_o						
Affected Vers	sion(s): * Up to (i	ncluding)	2.0.0				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in DgCult Exquisite PayPal Donation plugin <= v2.0.0 versions. <b>CVE ID : CVE-2023-</b>	N/A	A-EXQ-EXQU- 170523/121		
Scripting')			23785				
Vendor: eye	es_only_user_acc	ess_short	tcode_project				
Product: eye	es_only_user_ac	cess_shor	rtcode				
Affected Vers	sion(s): * Up to (i	ncluding)	1.8.2				
Improper Neutralizat ion of Input During Web Page	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Thom Stark Eyes Only: User Access	N/A	A-EYE-EYES- 170523/122		
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10							

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Shortcode plugin <= 1.8.2 versions. CVE ID : CVE-2023- 25786		
Vendor: F5					
Product: big	g-ip_access_poli	cy_manag	ger		
Affected Ver	sion(s): 14.1.5				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/123
Affected Ver	sion(s): 15.1.4.1			Γ	
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization.	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/124
			Note: Software versions which have reached End of		

0-1

1-2

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 16.1.2			1	
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/125
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 17.0.0				
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/126

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- 29163					
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/127			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/128			

0-1

1-2

2-3

**3-4 4-5** Page **71** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 27378		
Improper Enforceme nt of Message Integrity During Transmissi on in a Communic ation Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 22372</b>	https://my.f 5.com/mana ge/s/article/ K000132522	A-F5-BIG 170523/129
Improper Certificate Validation	03-May-2023	5.9	An improper certificate validation vulnerabil ity exists in the BIG- IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000132539	A-F5-BIG 170523/130

0-1

1-2

2-33-44-5Page 72 of 1106

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24461		
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	-
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/131
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	29163 A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/132

0-1

1-2

2-33-44-5Page 73 of 1106

5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/133
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to (including)	14.1.5	
Improper Enforceme nt of Message Integrity During Transmissi on in a Communic ation Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 22372</b>	https://my.f 5.com/mana ge/s/article/ K000132522	A-F5-BIG 170523/134

0-1

1-2

2-33-44-5Page 74 of 1106

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	03-May-2023 sion(s): From (in	5.9 cluding) 1	An improper certificate validation vulnerabil ity exists in the BIG- IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 24461 5.1.0 Up to (excluding)	https://my.f 5.com/mana ge/s/article/ K000132539	A-F5-BIG 170523/135
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/136
Improper Limitation of a Pathname to a Restricted Directory	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/137

0-1

1-2

2-33-44-5Page 75 of 1106

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/138
			CVE ID : CVE-2023- 27378		

0-1

1-2

2-33-44-5Page 76 of 1106

5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Improper Enforceme nt of Message Integrity During Transmissi on in a Communic ation Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 22372</b>	https://my.f 5.com/mana ge/s/article/ K000132522	A-F5-BIG 170523/139				
Improper Certificate Validation	03-May-2023	5.9	An improper certificate validation vulnerabil ity exists in the BIG- IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 24461	https://my.f 5.com/mana ge/s/article/ K000132539	A-F5-BIG 170523/140				
Affected Ver	Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4								
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/141				

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/142
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/143

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')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>		
Affected Ver	aion (a). From (in	aludina) 1	27378	1612	
Affected Ver	sion(s): From (in	cluding) 1	.6.1.0 Up to (including)	10.1.3	
Improper Enforceme nt of Message Integrity During Transmissi on in a Communic ation Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 22372</b>	https://my.f 5.com/mana ge/s/article/ K000132522	A-F5-BIG 170523/144
Improper Certificate Validation	03-May-2023	5.9	An improper certificate validation vulnerabil ity exists in the BIG- IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP	https://my.f 5.com/mana ge/s/article/ K000132539	A-F5-BIG 170523/145

0-1

1-2

2-3

**3-4 4-5** Page **79** of **1106**  8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 24461		
Affected Ver	sion(s): From (in	cluding) 1	7.0.0 Up to (excluding)	17.1.0.1	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/146
Improper Neutralizat ion of Input During Web Page	03-May-2023	6.1	28406 Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/147

0-1

1-2

2-33-44-5Page 80 of 1106

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
Affected Ver	gion(g); Enorm (in	oludina) 1	CVE ID : CVE-2023- 27378	1710	
Affected Ver	sion(s): From (in	cluding) 1	7.0.0 Up to (including)	17.1.0	
Improper Enforceme nt of Message Integrity During Transmissi on in a Communic ation Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 22372</b>	https://my.f 5.com/mana ge/s/article/ K000132522	A-F5-BIG 170523/148
Improper Certificate Validation	03-May-2023	5.9	An improper certificate validation vulnerabil ity exists in the BIG- IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note:	https://my.f 5.com/mana ge/s/article/ K000132539	A-F5-BIG 170523/149

0-1

1-2

2-3

**3-4 4-5** Page **81** of **1106**  7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 24461		
Affected Ver	sion(s): From (in	cluding) 7	.2.2 Up to (excluding) 7	.2.4.1	
Improper Enforceme nt of Message Integrity During Transmissi on in a Communic ation Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 22372</b>	https://my.f 5.com/mana ge/s/article/ K000132522	A-F5-BIG 170523/150
Improper Certificate Validation	03-May-2023	5.9	An improper certificate validation vulnerabil ity exists in the BIG- IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000132539	A-F5-BIG 170523/151

0-1

1-2

2-3

**3-4 4-5** Page **82** of **1106**  5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24461		
	g-ip_advanced_f	irewall_m	lanager		
Affected Ver	sion(s): 14.1.5				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 24594	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/152
Affected Ver	sion(s): 15.1.4.1		L	I	
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/153

0-1

1-2

2-3

**3-4 4-5** Page **83** of **1106**  6-7 7-8

5-6

		CVE ID : CVE-2023- 24594		
sion(s): 16.1.2				
03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/154
sion(s): 17.0.0			I	I
03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/155
	03-May-2023 ion(s): 17.0.0 03-May-2023	03-May-2023 7.5 ion(s): 17.0.0 03-May-2023 7.5	03-May-2023 7.5 When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>24594</b> ion(s): 17.0.9 03-May-2023 7.5 When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>29163</b>	03-May-20237.5When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization.https://my.f S.com/mana ge/s/article/ K00013313203-May-20237.5Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.https://my.f S.com/mana ge/s/article/ K000133132ion(s): 17.0.0Versions which have reached End of Technical Support (EoTS) are not evaluated.https://my.f S.com/mana ge/s/article/ K000133132ion(s): 17.0.0Versions which have reached End of Technical Support (EoTS) are not evaluated.https://my.f S.com/mana ge/s/article/ K0013313203-May-20237.5When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023-

0-1

1-2

2-33-44-5Page 84 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/156
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/157

0-1

1-2

2-3

**3-4 4-5** Page **85** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/158
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/159
			Note: Software versions which have		

0-1

1-2

2-33-44-5Page 86 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/160
Affected Ver	sion(s): From (in	cluding) 1	5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/161

0-1

1-2

2-3

**3-4 4-5** Page **87** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/162
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/163

0-1

1-2

2-3

**3-4 4-5** Page **88** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	6.1.0 Up to (excluding)	16.1.3.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/164
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/165

0-1

1-2

2-3

**3-4 4-5** Page **89** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/166
Affected Ver	sion(s): From (in	cluding) 1	7.0.0 Up to (excluding)	17.1.0.1	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/167

0-1

1-2

2-3

**3-4 4-5** Page **90** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/168
	g-ip_advanced_w	veb_appli	cation_firewall		
	sion(s): 14.1.5				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/169

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause an increase in CPU or SSL accelerator resource utilization.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 15.1.4.1			1	
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 24594	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/170
Affected Ver	sion(s): 16.1.2				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/171

0-1

1-2

2-33-44-5Page 92 of 1106

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL accelerator resource utilization.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 17.0.0				
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/172
Affected Ver	sion(s): From (in	cluding) 1	3.1.0 Up to (including)	13.1.5	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/173

0-1

1-2

2-33-44-5Page **93** of **1106** 

7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Descriptio	on & CVE ID		Patch		NCIIP	C ID
			attacker d control wl informatic obtained.	hat on is					
			Note: Soft versions v reached E Technical (EoTS) are evaluated. <b>CVE ID : C</b> 28406	vhich have nd of Support e not					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple r cross-site (XSS) vulr exist in un pages of th Configurat which allo attacker to JavaScript context of currently user. Note versions v reached E Technical (EoTS) are evaluated. <b>CVE ID : C</b> 27378	scripting nerabilities ndisclosed he BIG-IP tion utility ow an o run c in the the logged-in e: Software which have nd of Support e not	y re e	https://m 5.com/ma ge/s/arti K000132	ana cle/	A-F5-BIG 170523/	
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to	(excludin	ıg) 1	4.1.5.4			
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,		et	https://n 5.com/ma ge/s/artio K201451	ana cle/	A-F5-BIG 170523/	
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 **94** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/176
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/177

0-1

1-2

2-3

**3-4 4-5** Page **95** of **1106**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>		
Affected Ver	sion(s): From (in	cluding) 1	27378 5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/178
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/179

0-1

1-2

2-3

**3-4 4-5** Page **96** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is limited and the attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/180
Affected Ver	sion(s): From (in	cluding) 1	27378 6.1.0 Up to (excluding)	16.1.3.4	
Missing Release of Memory after	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/181
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4 4-5 5-6	6-7 7-8	3 8-9 <mark>9-10</mark>

Page **97** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>29163</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/182
_			28406		
Improper Neutralizat ion of Input	03-May-2023	6.1	Multiple reflected cross-site scripting	https://my.f 5.com/mana	A-F5-BIG 170523/183

0-1

1-2

2-3

**3-4 4-5** Page **98** of **1106**  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')			(XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	ge/s/article/ K000132726	
Affected Ver	<mark>sion(s): From (in</mark>	cluding) 1	7.0.0 Up to (excluding)	17.1.0.1	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/184

0-1

1-2

2-33-44-5Page 99 of 1106

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/185
Product: big	g-ip_analytics				
Affected Ver	sion(s): 14.1.5			1	
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/186
			versions which have reached End of Technical Support (EoTS) are not evaluated.		

0-1

1-2

**2-3** 3-4 4-5 Page **100** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 15.1.4.1				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/187
Affected Ver	sion(s): 16.1.2			<u> </u>	
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/188

0-1

1-2

2-33-44-5Page 101 of 1106

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Ver	Affected Version(s): 17.0.0							
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/189			
Affected Ver	sion(s): From (in	cluding) 1	.3.1.0 Up to (including)	13.1.5				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/190			

0-1

1-2

2-33-44-5Page 102 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/191
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/192

0-1

1-2

2-33-44-5Page 103 of 1106

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/193
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/194

0-1

1-2

**2-3** 3-4 4-5 Page **104** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/195
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/196
			Note: Software versions which have		

0-1

1-2

**2-3** 3-4 4-5 Page **105** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/197
Affected Ver	sion(s): From (in	cluding) 1	6.1.0 Up to (excluding)	16.1.3.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/198

0-1

1-2

**2-3** 3-4 4-5 Page **106** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/199
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/200

0-1

1-2

**2-3** 3-4 4-5 Page **107** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	7.0.0 Up to (excluding)	17.1.0.1	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/201
			versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>		
Improper Neutralizat ion of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/202

0-1

1-2

**2-3** 3-4 4-5 Page **108** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>		
	g-ip_application	_accelera	tion_manager		
Affected Ver	sion(s): 14.1.5			ſ	
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 24594	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/203
Affected Ver	sion(s): 15.1.4.1			1	l
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/204

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			SSL accelerator resource utilization.				
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.				
			CVE ID : CVE-2023- 24594				
Affected Ver	sion(s): 16.1.2						
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 24594	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/205		
Affected Version(s): 17.0.0							
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note:	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/206		

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 29163		
Affected Ver	sion(s): From (in	cluding) 1	3.1.0 Up to (including)	13.1.5	L
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/207
Improper Neutralizat ion of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/208

0-1

1-2

2-33-44-5Page 111 of 1106

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>		
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/209
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/210

0-1

1-2

2-33-44-5Page 112 of 1106

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/211
Affected Ver	<mark>sion(s): From (in</mark>	cluding) 1	27378 5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/212
CVSS Scoring S	Scale 0-1	L-2 2-3	<b>3-4 4-5 5-6</b>	6-7 7-8	8 8-9 9-10

Page 113 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/213
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/214

0-1

1-2

2-33-44-5Page 114 of 1106

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>		
Affected Ver	sion(s): From (in	cluding) 1	27378 6.1.0 Up to (excluding)	16.1.3.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/215
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/216

0-1

1-2

2-33-44-5Page 115 of 1106

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			information is limited and the attacker does not control what information is obtained.				
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/217		
Affected Ver	<mark>sion(s): From (in</mark>	cluding) 1	7.0.0 Up to (excluding)	17.1.0.1	<u> </u>		
Improper Limitation of a Pathname	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/218		
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
to a Restricted Directory ('Path Traversal')			Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/219

0-1

1-2

2-33-44-5Page 117 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2023- 27378							
	Product: big-ip_application_security_manager									
Affected Ver	sion(s): 14.1.5									
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 24594	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/220					
Affected Ver	sion(s): 15.1.4.1			I	L					
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/221					

0-1

1-2

**2-3** 3-4 4-5 Page **118** of **1106**  6-7 7-8

5-6

Affected Version(s): 16.1.2CVE ID : CVE-2023- 24594Affected Version(s): 16.1.2	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Uncontroll ed Resource Consumpti on03-May-20237.5When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization.https://my.f 5.com/mana ge/s/article/ K00133132A-F5-BIG 170523/222Affected Version(s): 17.0.07.5When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to eather on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached Effective Lifetime7.5When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- to immate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023-https://my.f A-F5-BIG 170523/222								
Uncontroll ed Resource Consumpti on03-May-20237.54is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization.https://my.f S.com/mana ge/s/article/ K000133132A-F5-BIG A-F5-BIG 170523/222Missing Netesource to nVere user and the content of the c	Affected Vers	sion(s): 16.1.2						
Missing Release of Memory after Effective Lifetime03-May-20237.5When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.Https://my.f 5.com/mana ge/s/article/ K20145107A-F5-BIG 170523/223	ed Resource Consumpti	03-May-2023	7.5	is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>	5.com/mana ge/s/article/			
Missing Release of Memory after Effective Lifetime03-May-20237.5with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.https://my.fA-F5-BIG170523/223170523/223	Affected Vers	sion(s): 17.0.0						
29103	Missing Release of Memory after 							

0-1

1-2

2-33-44-5Page 119 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/224
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/225

0-1

1-2

2-33-44-5Page 120 of 1106

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/226
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/227
			Note: Software versions which have		

0-1

1-2

2-33-44-5Page 121 of 1106

5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/228
Affected Ver	sion(s): From (in	cluding) 1	5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/229

0-1

1-2

2-33-44-5Page 122 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/230
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/231

0-1

1-2

2-33-44-5Page 123 of 1106

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	6.1.0 Up to (excluding)	16.1.3.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/232
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/233

0-1

1-2

**2-3** 3-4 4-5 Page **124** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/234
Affected Ver	sion(s): From (in	cluding) 1	7.0.0 Up to (excluding)	17.1.0.1	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/235

0-1

1-2

2-33-44-5Page 125 of 1106

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/236
Product: big	g-ip_application	_visibility	_and_reporting		
Affected Ver	sion(s): 14.1.5				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/237

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			can cause an increase in CPU or SSL accelerator resource utilization.					
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.					
			CVE ID : CVE-2023- 24594					
Affected Ver	sion(s): 15.1.4.1			1				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/238			
Affected Ver	Affected Version(s): 16.1.2							
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/239			

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL accelerator resource utilization.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 17.0.0				
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/240
Affected Ver	sion(s): From (in	cluding) 1	3.1.0 Up to (including)	13.1.5	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/241

0-1

1-2

**2-3** 3-4 4-5 Page **128** of **1106**  8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			attacker does not control what information is obtained.					
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 27378	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/242			
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4								
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/243			
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4 4-5 5-6	6-7 7-8	8 8-9 9-10			

Page 129 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/244
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/245

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>		
Affected Ver	sion(s): From (in	cluding) 1	27378 5.1.0 Up to (excluding)	15182	
				13.1.0.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/246
			29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/247

0-1

1-2

2-33-44-5Page 131 of 1106

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			information is limited and the attacker does not control what information is obtained.					
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 27378	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/248			
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4								
Missing Release of Memory after	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/249			
CVSS Scoring S	Scale 0-1 C	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>132</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>29163</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/250
Improper Neutralizat	03-May-2023	6.1		https://my.f	A-F5-BIG
ion of Input	55 May 2020		Multiple reflected cross-site scripting	5.com/mana	170523/251

0-1

1-2

2-33-44-5Page 133 of 1106

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')			(XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	ge/s/article/ K000132726	
Affected Vers	sion(s): From (in	cluding) 1	7.0.0 Up to (excluding)	17.1.0.1	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/252

0-1

1-2

**2-3** 3-4 4-5 Page **134** of **1106**  5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/253
Product: big	g-ip_carrier-grad	de nat	2,010		
	sion(s): 14.1.5	-			
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/254

0-1

1-2

2-33-44-5Page 135 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 15.1.4.1				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/255
Affected Ver	sion(s): 16.1.2			1	l
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/256

0-1

1-2

**2-3** 3-4 4-5 Page **136** of **1106**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 17.0.0				•
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/257
Affected Ver	sion(s): From (in	cluding) 1	3.1.0 Up to (including)	13.1.5	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/258

0-1

1-2

2-33-44-5Page 137 of 1106

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/259
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/260

0-1

1-2

**2-3** 3-4 4-5 Page **138** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/261
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/262

0-1

1-2

**2-3** 3-4 4-5 Page **139** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/263
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/264
			Note: Software versions which have		

0-1

1-2

**2-3** 3-4 4-5 Page **140** of **1106**  5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/265
Affected Ver	sion(s): From (in	cluding) 1	6.1.0 Up to (excluding)	16.1.3.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/266

0-1

1-2

2-33-44-5Page 141 of 1106

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/267
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/268

0-1

1-2

2-33-44-5Page 142 of 1106

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	7.0.0 Up to (excluding)	17.1.0.1	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/269
			versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>		
Improper Neutralizat ion of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/270

0-1

1-2

2-33-44-5Page 143 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>		
Product: big	g-ip_ddos_hybrio	d_defend	er		
Affected Ver	sion(s): 14.1.5				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/271
Affected Ver	sion(s): 15.1.4.1		L	I	
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/272

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL accelerator resource utilization.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 16.1.2				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 24594	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/273
Affected Ver	sion(s): 17.0.0				
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note:	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/274

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 29163		
Affected Ver	sion(s): From (in	cluding) 1	3.1.0 Up to (including)	13.1.5	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/275
Improper Neutralizat ion of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/276

0-1

1-2

**2-3** 3-4 4-5 Page **146** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>		
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/277
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/278

0-1

1-2

**2-3** 3-4 4-5 Page **147** of **1106**  5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/279
Affected Vers	sion(s): From (in	cluding) 1	5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/280
CVSS Scoring S	Scale 0-1	L-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
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/281
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/282

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>		
Affected Ver	sion(s): From (in	cluding) 1	27378 .6.1.0 Up to (excluding)	16.1.3.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/283
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/284

0-1

1-2

**2-3** 3-4 4-5 Page **150** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is limited and the attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/285
Affected Ver	<mark>sion(s): From (in</mark>	cluding) 1	27378 7.0.0 Up to (excluding)	17.1.0.1	
Improper Limitation of a Pathname	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/286
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
to a Restricted Directory ('Path Traversal')			Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/287

0-1

1-2

2-33-44-5Page 152 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			CVE ID : CVE-2023- 27378						
	Product: big-ip_domain_name_system								
Affected Ver	sion(s): 14.1.5			Γ	Γ				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 24594	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/288				
Affected Ver	sion(s): 15.1.4.1		<u> </u>		I				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/289				

0-1

1-2

2-33-44-5Page 153 of 1106

6-7 7-8

5-6

1.2	CVE ID : CVE-2023- 24594When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or		
	is configured on a Virtual Server, undisclosed traffic can cause an		
	is configured on a Virtual Server, undisclosed traffic can cause an		
023 7.5	Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 24594	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/290
0.0			I
023 7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/291
		023 <b>7.5</b> undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>29163</b>	0237.5undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.https://my.f 5.com/mana ge/s/article/ K201451070237.5End of Technical Support (EoTS) are not evaluated.https://my.f 5.com/mana ge/s/article/ K20145107

0-1

1-2

**2-3** 3-4 4-5 Page **154** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	03-May-2023	8.8	When DNS is provisioned, an authenticated remote command execution vulnerability exists in DNS iQuery mesh. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28742</b>	https://my.f 5.com/mana ge/s/article/ K000132972	A-F5-BIG 170523/292
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/293

0-1

1-2

2-33-44-5Page 155 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/294
Affected ver	sion(s): From (in	ciuding) I	4.1.0 Up to (excluding)	14.1.5.4	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	03-May-2023	8.8	When DNS is provisioned, an authenticated remote command execution vulnerability exists in DNS iQuery mesh.	https://my.f 5.com/mana ge/s/article/ K000132972	A-F5-BIG 170523/295

0-1

1-2

**2-3** 3-4 4-5 Page **156** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28742		
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/296
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/297

0-1

1-2

2-33-44-5Page 157 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/298
	sion(s): From (in	cluding) 1	5.1.0 Up to (excluding)	15.1.8.2	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	03-May-2023	8.8	When DNS is provisioned, an authenticated remote command execution vulnerability exists in DNS iQuery mesh.	https://my.f 5.com/mana ge/s/article/ K000132972	A-F5-BIG 170523/299

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28742		
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/300
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/301

0-1

1-2

**2-3** 3-4 4-5 Page **159** of **1106**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is obtained. Note: Software		
			versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/302
Affected Ver	sion(s): From (in	cluding) 1	6.1.0 Up to (excluding)	16.1.3.4	
Improper Neutralizat ion of Special Elements used in an OS Command	03-May-2023	8.8	When DNS is provisioned, an authenticated remote command execution	https://my.f 5.com/mana ge/s/article/ K000132972	A-F5-BIG 170523/303

0-1

1-2

**2-3** 3-4 4-5 Page **160** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			vulnerability exists in DNS iQuery mesh. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28742</b>		
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/304
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/305

0-1

1-2

2-33-44-5Page 161 of 1106

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			limited and the attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/306
Affected Ver	sion(s): From (in	cluding) 1	27378 7.0.0 Up to (excluding)	17.1.0.1	
Improper Neutralizat ion of Special Elements	03-May-2023	8.8	When DNS is provisioned, an authenticated remote command	https://my.f 5.com/mana ge/s/article/ K000132972	A-F5-BIG 170523/307
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
used in an OS Command ('OS Command Injection')			execution vulnerability exists in DNS iQuery mesh.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>		
			28742		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/308
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		

0-1

1-2

2-33-44-5Page 163 of 1106

5-6

6-7 7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/309
Product: big	g-ip_edge_gatew	ay			
Affected Ver	sion(s): 14.1.5				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/310
			reached End of Technical Support (EoTS) are not evaluated.		

0-1

1-2

2-33-44-5Page 164 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 15.1.4.1				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/311
Affected Ver	sion(s): 16.1.2			L	l
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/312

0-1

1-2

**2-3** 3-4 4-5 Page **165** of **1106**  5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 17.0.0				•
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/313
Affected Ver	sion(s): From (in	cluding) 1	.3.1.0 Up to (including)	13.1.5	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/314

0-1

1-2

**2-3** 3-4 4-5 Page **166** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/315
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/316

0-1

1-2

**2-3** 3-4 4-5 Page **167** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/317
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/318

0-1

1-2

**2-3** 3-4 4-5 Page **168** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/319
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/320
			Note: Software versions which have		

0-1

1-2

**2-3** 3-4 4-5 Page **169** of **1106**  5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/321
Allected ver	sion(s): From (m		6.1.0 Up to (excluding)	10.1.3.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/322

0-1

1-2

2-33-44-5Page 170 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/323
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/324

0-1

1-2

2-33-44-5Page 171 of 1106

6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	7.0.0 Up to (excluding)	17.1.0.1	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/325
			versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/326

0-1

1-2

2-33-44-5Page 172 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>		
Product: big	g-ip_fraud_prote	ction_ser	vice		
Affected Ver	sion(s): 14.1.5			1	
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/327
Affected Ver	sion(s): 15.1.4.1		I	l	l
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/328

0-1

1-2

2-33-44-5Page 173 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL accelerator resource utilization.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 16.1.2				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 24594	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/329
Affected Ver	sion(s): 17.0.0		L	<u> </u>	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note:	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/330

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 29163		
Affected Ver	sion(s): From (in	cluding) 1	3.1.0 Up to (including)	13.1.5	L
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/331
Improper Neutralizat ion of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/332

0-1

1-2

2-33-44-5Page 175 of 1106

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>		
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/333
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/334

0-1

1-2

2-33-44-5Page 176 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/335
Affected Vers	<mark>sion(s): From (in</mark>	cluding) 1	5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/336
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Page 177 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/337
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/338

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>		
Affected Ver	sion(s): From (in	cluding) 1	27378 .6.1.0 Up to (excluding)	16134	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/339
			29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/340

0-1

1-2

**2-3** 3-4 4-5 Page **179** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is limited and the attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/341
Affected Ver	<mark>sion(s): From (in</mark>	cluding) 1	27378 7.0.0 Up to (excluding)	17.1.0.1	
Improper Limitation of a Pathname	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/342
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b>	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')			Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/343

0-1

1-2

2-33-44-5Page 181 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 27378		
	g-ip_global_traff	ic_manag	er		
Affected Ver	sion(s): 14.1.5				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 24594	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/344
Affected Ver	sion(s): 15.1.4.1		L	I	
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/345

0-1

1-2

2-33-44-5Page 182 of 1106

5-6

on(s): 16.1.2		CVE ID : CVE-2023-		
on(s): 16.1.2		24594		
03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/346
on(s): 17.0.0				L
03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/347
0	on(s): 17.0.0 )3-May-2023	on(s): 17.0.0 03-May-2023 7.5	D3-May-20237.5Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization.D3-May-20237.5Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.cve iD : CVE-2023- 24594con(s): 17.0.0When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	D3-May-20237.5Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization.https://my.f 5.com/mana ge/s/article/ K000133132D3-May-20237.5Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.https://my.f 5.com/mana ge/s/article/ K000133132on(s): 17.0.0When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.https://my.f S.com/mana ge/s/article/ K20145107

0-1

1-2

**2-3** 3-4 4-5 Page **183** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/348
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/349

0-1

1-2

**2-3** 3-4 4-5 Page **184** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/350
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/351
			Note: Software versions which have		

0-1

1-2

**2-3** 3-4 4-5 Page **185** of **1106**  5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/352
Affected Ver	sion(s): From (in	cluding) 1	5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/353

0-1

1-2

**2-3** 3-4 4-5 Page **186** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/354
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/355

0-1

1-2

**2-3** 3-4 4-5 Page **187** of **1106**  6-7

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	6.1.0 Up to (excluding)	16.1.3.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/356
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/357

0-1

1-2

**2-3** 3-4 4-5 Page **188** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/358
Affected Ver	sion(s): From (in	cluding) 1	7.0.0 Up to (excluding)	17.1.0.1	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/359

0-1

1-2

**2-3** 3-4 4-5 Page **189** of **1106**  5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			control what information is obtained.				
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.				
			CVE ID : CVE-2023- 28406				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/360		
Product: big-ip_link_controller							
	sion(s): 14.1.5						
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/361		

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause an increase in CPU or SSL accelerator resource utilization.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 15.1.4.1			1	
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/362
Affected Ver	sion(s): 16.1.2		- 107 1		
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/363

0-1

1-2

2-33-44-5Page 191 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL accelerator resource utilization.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 17.0.0				
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/364
Affected Ver	sion(s): From (in	cluding) 1	3.1.0 Up to (including)	13.1.5	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/365

0-1

1-2

2-33-44-5Page 192 of 1106

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/366
Affected Vers	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/367
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 193 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/368
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/369

0-1

1-2

**2-3** 3-4 4-5 Page **194** of **1106**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>		
Affected Ver	sion(s): From (in	cluding) 1	27378 5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/370
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/371

0-1

1-2

**2-3** 3-4 4-5 Page **195** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is limited and the attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/372
Affected Ver	sion(s): From (in	cluding) 1	27378 6.1.0 Up to (excluding)	16.1.3.4	
Missing Release of Memory after	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/373
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Page 196 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	29163 A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/374
Improper Neutralizat				https://my.f	A-F5-BIG
ion of Input	03-May-2023	6.1	Multiple reflected cross-site scripting	5.com/mana	170523/375

0-1

1-2

**2-3** 3-4 4-5 Page **197** of **1106**  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')			(XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	ge/s/article/ K000132726	
Affected Vers	sion(s): From (in	cluding) 1	7.0.0 Up to (excluding)	17.1.0.1	l
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/376

0-1

1-2

**2-3** 3-4 4-5 Page **198** of **1106**  5-6

6-7

7-8

8-9 9-10

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		CVE ID : CVE-2023- 28406		
03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/377
y-in local traffic	' manage			
sion(s): 14.1.5	_manage	•		
03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/378
	03-May-2023 g-ip_local_traffic sion(s): 14.1.5	o3-May-2023       6.1         g-ip_local_traffic_manage         sion(s): 14.1.5	Image: constraint of the second sec	Image: Constraint of the series of the ser

0-1

1-2

2-3 3-4 4-5 Page **199** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 15.1.4.1				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/379
Affected Ver	sion(s): 16.1.2		L		
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/380

0-1

1-2

**2-3** 3-4 4-5 Page **200** of **1106**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 17.0.0				•
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/381
Affected Ver	sion(s): From (in	cluding) 1	3.1.0 Up to (including)	13.1.5	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/382

0-1

1-2

2-33-44-5Page 201 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/383
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/384

0-1

1-2

2-33-44-5Page 202 of 1106

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/385
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/386

0-1

1-2

2-33-44-5Page 203 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/387
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/388
			Note: Software versions which have		

0-1

1-2

**2-3** 3-4 4-5 Page **204** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/389
Affected Ver	sion(s): From (in	cluding) 1	6.1.0 Up to (excluding)	16.1.3.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/390

0-1

1-2

**2-3** 3-4 4-5 Page **205** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/391
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/392

0-1

1-2

**2-3** 3-4 4-5 Page **206** of **1106**  8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	7.0.0 Up to (excluding)	17.1.0.1	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/393
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/394

0-1

1-2

**2-3** 3-4 4-5 Page **207** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>		
Product: big	g-ip_next_servic	e_proxy_f	or_kubernetes	<u> </u>	
Affected Ver	sion(s): 1.5.0				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/395
Product: big	g-ip_policy_enfo	rcement_	manager		
Affected Ver	sion(s): 14.1.5				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/396

0100 000118 00010	~ -			•••		
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
			increase in CPU or SSL accelerator resource utilization.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 15.1.4.1				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/397
Affected Ver	sion(s): 16.1.2				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/398

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL accelerator resource utilization.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 17.0.0				
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/399
Affected Ver	sion(s): From (in	cluding) 1	3.1.0 Up to (including)	13.1.5	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/400

0-1

1-2

2-33-44-5Page 210 of 1106

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/401
Affected Vers	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/402
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Page **211** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/403
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/404

0-1

1-2

2-33-44-5Page 212 of 1106

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>		
Affected Ver	sion(s): From (in	cluding) 1	27378 5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/405
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/406

0-1

1-2

2-33-44-5Page 213 of 1106

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is limited and the attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/407
Affected Ver	sion(s): From (in	cluding) 1	6.1.0 Up to (excluding)	16.1.3.4	
Missing Release of Memory after	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/408
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>214</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Effective					
Lifetime			value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>29163</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/409
Improper Neutralizat ion of	03-May-2023	6.1	Multiple reflected cross-site scripting	https://my.f 5.com/mana	A-F5-BIG 170523/410

0-1

1-2

2-33-44-5Page 215 of 1106

5-6 6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			(XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	ge/s/article/ K000132726	
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/411

0-1

1-2

**2-3** 3-4 4-5 Page **216** of **1106**  5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/412
Product: big	g-ip_ssl_orchest	rator			
Affected Ver	sion(s): 14.1.5				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/413

0-1

1-2

2-33-44-5Page 217 of 1106

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 15.1.4.1				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/414
Affected Ver	sion(s): 16.1.2			I	
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 24594	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/415

0-1

1-2

**2-3** 3-4 4-5 Page **218** of **1106**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 17.0.0				
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/416
Affected Ver	sion(s): From (in	cluding) 1	3.1.0 Up to (including)	13.1.5	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/417

0-1

1-2

2-33-44-5Page 219 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/418
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/419

0-1

1-2

**2-3** 3-4 4-5 Page **220** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/420
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/421

0-1

1-2

2-33-44-5Page 221 of 1106

5-6

7-8

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/422
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/423
			Note: Software versions which have		

0-1

1-2

2-33-44-5Page 222 of 1106

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/424
Affected Ver	sion(s): From (in	cluding) 1	6.1.0 Up to (excluding)	16.1.3.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/425

0-1

1-2

2-33-44-5Page 223 of 1106

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/426
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/427

0-1

1-2

**2-3** 3-4 4-5 Page **224** of **1106**  6-7

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	7.0.0 Up to (excluding)	17.1.0.1	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/428
			(EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/429

0-1

1-2

2-33-44-5Page 225 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>		
Product: big	g-ip_webacceler	ator			
Affected Ver	sion(s): 14.1.5				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 24594	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/430
Affected Ver	sion(s): 15.1.4.1			I	
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/431

0-1

1-2

**2-3** 3-4 4-5 Page **226** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL accelerator resource utilization.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 24594		
Affected Ver	sion(s): 16.1.2				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 24594	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/432
Affected Ver	sion(s): 17.0.0				
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note:	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/433

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 29163		
Affected Ver	sion(s): From (in	cluding) 1	3.1.0 Up to (including)	13.1.5	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/434
Improper Neutralizat ion of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/435

0-1

1-2

**2-3** 3-4 4-5 Page **228** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>		
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/436
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/437

0-1

1-2

**2-3** 3-4 4-5 Page **229** of **1106**  5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/438
Affected Vers	sion(s): From (in	cluding) 1	5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/439
CVSS Scoring S	Scale 0-1	L-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
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/440
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/441

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>		
			27378		
Affected Ver	sion(s): From (in	cluding) 1	6.1.0 Up to (excluding)	16.1.3.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/442
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/443

0-1

1-2

2-33-44-5Page 232 of 1106

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is limited and the attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/444
Affected Ver	<mark>sion(s): From (</mark> in	cluding) 1	27378 7.0.0 Up to (excluding)	17.1.0.1	
Improper Limitation of a Pathname	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/445
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
to a Restricted Directory ('Path Traversal')			Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.		
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/446

0-1

1-2

**2-3** 3-4 4-5 Page **234** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 27378		
Product: big	g-ip_websafe				
Affected Ver	sion(s): 14.1.5				
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> 24594	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/447
Affected Ver	sion(s): 15.1.4.1				<u> </u>
Uncontroll ed Resource Consumpti on	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/448

0-1

1-2

2-33-44-5Page 235 of 1106

6-7 7-8

5-6

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		CVE ID : CVE-2023- 24594		
sion(s): 16.1.2				
03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 24594</b>	https://my.f 5.com/mana ge/s/article/ K000133132	A-F5-BIG 170523/449
sion(s): 17.0.0				1
03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29163</b>	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/450
	03-May-2023 sion(s): 17.0.0 03-May-2023	03-May-2023 7.5 sion(s): 17.0.0 03-May-2023 7.5	ion(s): 16.1.224594sion(s): 16.1.2When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization.03-May-20237.5Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.stor(s): 17.00When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.03-May-20237.5Verein UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 29163	ision(s): 16.1.2sion(s): 16.1.203-May-20237.5Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization.03-May-20237.57.5Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.sion(s): 17.0.0Virtual Server, undisclosed traffic can cause an 

0-1

1-2

2-33-44-5Page 236 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/451
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/452

0-1

1-2

2-33-44-5Page 237 of 1106

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	4.1.0 Up to (excluding)	14.1.5.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/453
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/454
			Note: Software versions which have		

0-1

1-2

**2-3** 3-4 4-5 Page **238** of **1106**  5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023</b> -		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	28406 Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 27378	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/455
Affected Ver	sion(s): From (in	cluding) 1	5.1.0 Up to (excluding)	15.1.8.2	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/456

0-1

1-2

2-33-44-5Page 239 of 1106

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 28406</b>	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/457
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/458

0-1

1-2

**2-3** 3-4 4-5 Page **240** of **1106**  8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 27378		
Affected Ver	sion(s): From (in	cluding) 1	6.1.0 Up to (excluding)	16.1.3.4	
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K20145107	A-F5-BIG 170523/459
			CVE ID : CVE-2023- 29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/460

0-1

1-2

2-33-44-5Page 241 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28406		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023-</b> <b>27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/461
Affected Ver	sion(s): From (in	cluding) 1	7.0.0 Up to (excluding)	17.1.0.1	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not	https://my.f 5.com/mana ge/s/article/ K000132768	A-F5-BIG 170523/462

0-1

1-2

2-33-44-5Page 242 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			control what information is obtained.				
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.				
			CVE ID : CVE-2023- 28406				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 27378</b>	https://my.f 5.com/mana ge/s/article/ K000132726	A-F5-BIG 170523/463		
Product: big-iq_centralized_management							
	sion(s): From (in	cluding) 8	8.0.0 Up to (excluding) 8	.3.0			
Unrestricte d Upload of File with Dangerous Type	03-May-2023	5.4	An authenticated attacker granted a Viewer or Auditor role on a BIG-IQ can	https://my.f 5.com/mana ge/s/article/ K000132719	A-F5-BIG 170523/464		

 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
Decident			upload arbitrary files using an undisclosed iControl REST endpoint. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 29240</b>		
	inx_api_connect			5.0	
Affected Ver	sion(s): From (in	cluding) 1	.0.0 Up to (excluding) 1	.5.0	
Authorizati on Bypass Through User- Controlled Key	03-May-2023	8.1	NGINX Management Suite may allow an authenticated attacker to gain access to configuration objects outside of their assigned environment. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28656	https://my.f 5.com/mana ge/s/article/ K000133417	A-F5-NGIN- 170523/465
Incorrect Default	03-May-2023	7.1		https://my.f 5.com/mana	A-F5-NGIN- 170523/466

0-1

1-2

**2-3** 3-4 4-5 Page **244** of **1106**  5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permission s			NGINX Management Suite default file permissions are set such that an authenticated attacker may be able to modify sensitive files on NGINX Instance Manager and NGINX API Connectivity Manager.	ge/s/article/ K000133233	
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 28724		
	inx_instance_ma	U			
Affected Ver	sion(s): From (in	cluding) 2	.0.0 Up to (excluding) 2	.9.0	
Authorizati on Bypass Through User- Controlled Key	03-May-2023	8.1	NGINX Management Suite may allow an authenticated attacker to gain access to configuration objects outside of their assigned environment.	https://my.f 5.com/mana ge/s/article/ K000133417	A-F5-NGIN- 170523/467
			Note: Software versions which have reached End of		

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 28656		
Incorrect Default Permission s	03-May-2023	7.1	NGINX Management Suite default file permissions are set such that an authenticated attacker may be able to modify sensitive files on NGINX Instance Manager and NGINX API Connectivity Manager. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023-	https://my.f 5.com/mana ge/s/article/ K000133233	A-F5-NGIN- 170523/468
Duadrat			28724		
_	inx_security_mo	_	.0.0 Up to (excluding) 1	2.0	
Alletted vel		ciuding) I			

0-1

1-2

2-33-44-5Page 246 of 1106

5-6

6-7

7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorizati on Bypass Through User- Controlled Key	03-May-2023	8.1	NGINX Management Suite may allow an authenticated attacker to gain access to configuration objects outside of their assigned environment. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. CVE ID : CVE-2023- 28656	https://my.f 5.com/mana ge/s/article/ K000133417	A-F5-NGIN- 170523/469
Incorrect Default Permission s	03-May-2023	7.1	NGINX Management Suite default file permissions are set such that an authenticated attacker may be able to modify sensitive files on NGINX Instance Manager and NGINX API Connectivity Manager. Note: Software versions which have	https://my.f 5.com/mana ge/s/article/ K000133233	A-F5-NGIN- 170523/470

0-1

1-2

**2-3** 3-4 4-5 Page **247** of **1106**  8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated.		
			CVE ID : CVE-2023- 28724		
Vendor: far	eharbor		L	I	
Product: far	reharbor				
Affected Vers	sion(s): * Up to (e	excluding)	3.6.7		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in FareHarbor FareHarbor for WordPress plugin <= 3.6.6 versions. <b>CVE ID : CVE-2023-</b> <b>25021</b>	N/A	A-FAR-FARE- 170523/471
Vendor: fast	tlinemedia			1	
Product: cu	stomizer_expor	t\/impor	t		
Affected Vers	sion(s): * Up to (e	excluding)	0.9.6		
Deserializa tion of Untrusted Data	08-May-2023	7.2	The Customizer Export/Import WordPress plugin before 0.9.6 unserializes user input provided via the settings, which could allow high privilege users such as admin to perform PHP Object Injection when a suitable gadget is present	N/A	A-FAS-CUST- 170523/472

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 1347		
Vendor: Fee	loraproject				
Product: ex	tra_packages_fo	r_enterpi	rise_linux		
Affected Ver	sion(s): 7.0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user- supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database. <b>CVE ID : CVE-2023- 30944</b>	https://moo dle.org/mod /forum/disc uss.php?d=4 46286, https://bugz illa.redhat.co m/show_bug .cgi?id=2188 606, http://git.m oodle.org/g w?p=moodle .git&a=searc h&h=HEAD& st=commit& s=MDL- 77187	A-FED-EXTR- 170523/473
Externally Controlled Reference to a Resource in Another Sphere	02-May-2023	5.3	The vulnerability was found Moodle which exists because the application allows a user to control path of the older to create in TinyMCE loaders. A remote user can send a specially crafted HTTP request and create arbitrary folders on the system. <b>CVE ID : CVE-2023-</b> <b>30943</b>	http://git.m oodle.org/g w?p=moodle .git&a=searc h&h=HEAD& st=commit& s=MDL- 77718, https://moo dle.org/mod /forum/disc uss.php?d=4 46285, https://bugz illa.redhat.co m/show_bug .cgi?id=2188 605	A-FED-EXTR- 170523/474

0-1

1-2

**2-3** 3-4 4-5 Page **249** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Vendor: fin	viz	I		I	L			
Product: sto	Product: stock_market_charts_from_finviz							
Affected Ver	sion(s): * Up to (i	ncluding)	1.0.1					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Moris Dov Stock market charts from finviz plugin <= 1.0.1 versions. <b>CVE ID : CVE-2023- 23809</b>	N/A	A-FIN-STOC- 170523/475			
Vendor: fire	ecask_like_\&_sl	nare_butt	on_project					
Product: fir	ecask_like_\&_s	hare_but	ton					
Affected Ver	sion(s): * Up to (i	ncluding)	1.1.5					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Alex Moss FireCask Like & Share Button plugin <= 1.1.5 versions. <b>CVE ID : CVE-2023-</b>	N/A	A-FIR-FIRE- 170523/476			
Scripting')			25783					
	_	-	z_system_project					
	od_ordering_ma	nagemen	t_system					
Affected Ver	sion(s): 1.0		A 1 1.00					
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	09-May-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Food Ordering Management System 1.0. Affected is an unknown function of the component Registration. The manipulation of the	N/A	A-FOO-FOOD- 170523/477			

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument username leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB- 228396. <b>CVE ID : CVE-2023-</b>		
			2594		
Vendor: For					
Product: for					
Affected Ver	sion(s): 7.2.0				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	03-May-2023	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE- 78] in FortiADC 7.2.0, 7.1.0 through 7.1.1 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. <b>CVE ID : CVE-2023- 27999</b>	https://forti guard.com/p sirt/FG-IR- 22-297	A-FOR-FORT- 170523/478
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	7.1	A relative path traversal [CWE-23] in Fortinet FortiADC version 7.2.0 and before 7.1.1 allows a privileged attacker to delete arbitrary directories from the underlying file	https://forti guard.com/p sirt/FG-IR- 23-069	A-FOR-FORT- 170523/479

0-1

1-2

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system via crafted CLI commands.		
			CVE ID : CVE-2023- 27993		
Affected Ver	sion(s): From (in	cluding) 5	.2.0 Up to (including) 7	.0.5	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	7.1	A relative path traversal [CWE-23] in Fortinet FortiADC version 7.2.0 and before 7.1.1 allows a privileged attacker to delete arbitrary directories from the underlying file system via crafted CLI commands. <b>CVE ID : CVE-2023- 27993</b>	https://forti guard.com/p sirt/FG-IR- 23-069	A-FOR-FORT- 170523/480
Affected Ver	sion(s): From (in	cluding) 7	.1.0 Up to (excluding) 7	.1.2	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	03-May-2023	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE- 78] in FortiADC 7.2.0, 7.1.0 through 7.1.1 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. <b>CVE ID : CVE-2023- 27999</b>	https://forti guard.com/p sirt/FG-IR- 22-297	A-FOR-FORT- 170523/481
Improper Limitation of a Pathname	03-May-2023	7.1	A relative path traversal [CWE-23] in Fortinet FortiADC version 7.2.0 and	https://forti guard.com/p sirt/FG-IR- 23-069	A-FOR-FORT- 170523/482

0-1

1-2

2-33-44-5Page 252 of 1106

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			before 7.1.1 allows a privileged attacker to delete arbitrary directories from the underlying file system via crafted CLI commands. <b>CVE ID : CVE-2023-</b> <b>27993</b>		
Product: for	rtinac				
Affected Ver	sion(s): From (in	cluding) 8	8.7.0 Up to (excluding) 9	.4.3	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	9	An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE- 79] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.2 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions in License Management would permit an authenticated attacker to trigger remote code execution via crafted licenses. <b>CVE ID : CVE-2023- 22637</b>	https://forti guard.com/p sirt/FG-IR- 23-013	A-FOR-FORT- 170523/483
Affected Ver	sion(s): From (in	cluding) 8	.7.0 Up to (including) 9	.2.7	
Use of Hard- coded Credentials	03-May-2023	7.8	A use of hard-coded credentials vulnerability [CWE- 798] in FortiNAC-F version 7.2.0, FortiNAC version	https://forti guard.com/p sirt/FG-IR- 22-520	A-FOR-FORT- 170523/484

Page 253 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.4.2 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions all versions may allow an authenticated attacker to access to the database via shell commands. <b>CVE ID : CVE-2023-</b>		
			26203		
Affected Vers	sion(s): From (in	cluding) 9	.4.0 Up to (excluding) 9	.4.3	
Use of Hard- coded Credentials	03-May-2023	7.8	A use of hard-coded credentials vulnerability [CWE- 798] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.2 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions may allow an authenticated attacker to access to the database via shell commands. <b>CVE ID : CVE-2023-</b> <b>26203</b>	https://forti guard.com/p sirt/FG-IR- 22-520	A-FOR-FORT- 170523/485
Product: for	rtinac-f				
Affected Vers	sion(s): 7.2.0				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	9	An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE- 79] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.2 and below, 9.2	https://forti guard.com/p sirt/FG-IR- 23-013	A-FOR-FORT- 170523/486
CVSS Scoring S	Scale 0-1	L-2 2-3	<b>3-4 4-5 5-6</b> Page <b>254</b> of <b>1106</b>	6-7 7-8	3 <u>8-9</u> <u>9-10</u>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions in License Management would permit an authenticated attacker to trigger remote code execution via crafted licenses. <b>CVE ID : CVE-2023-</b> <b>22637</b>		
Use of Hard- coded Credentials	03-May-2023	7.8	A use of hard-coded credentials vulnerability [CWE- 798] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.2 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions may allow an authenticated attacker to access to the database via shell commands. <b>CVE ID : CVE-2023-</b> <b>26203</b>	https://forti guard.com/p sirt/FG-IR- 22-520	A-FOR-FORT- 170523/487
Product: for	rtiproxy				
Affected Ver	sion(s): 1.0.0				
Out-of- bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13,	https://forti guard.com/p sirt/FG-IR- 22-475	A-FOR-FORT- 170523/488

0-1

1-2

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests. <b>CVE ID : CVE-2023- 22640</b>		
Affected Ver	sion(s): 1.1.0		22040		
Out-of- bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2,	https://forti guard.com/p sirt/FG-IR- 22-475	A-FOR-FORT- 170523/489

0-1

1-2

**2-3** 3-4 4-5 Page **256** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests. <b>CVE ID : CVE-2023- 22640</b>		
Affected Ver	sion(s): 1.2.0				
Out-of- bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests.	https://forti guard.com/p sirt/FG-IR- 22-475	A-FOR-FORT- 170523/490
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5-6 Page <b>257</b> of <b>1106</b>	6-7 7-8	3 8-9 <mark>9-10</mark>

Page 257 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22640		
Affected Ver	sion(s): 2.0.0			I	I
Out-of- bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests. <b>CVE ID : CVE-2023-</b> <b>22640</b>	https://forti guard.com/p sirt/FG-IR- 22-475	A-FOR-FORT- 170523/491
	worksplugins				
	ick_paypal_pay		<b>F F O</b> ( <b>A</b>		
	sion(s): * Up to (e	excluding)			
Improper Neutralizat ion of Input	02-May-2023	4.8	The Quick Paypal Payments WordPress plugin before 5.7.26.4 does	N/A	A-FUL-QUIC- 170523/492
CVSS Scoring S	Scale 0-1	L-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
During Web Page Generation ('Cross-site Scripting')			not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) CVE ID : CVE-2023- 1554		
Vendor: fun	admin			<u> </u>	
Product: fui	nadmin				
Affected Ver	sion(s): * Up to (i	ncluding)	3.2.3		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	6.1	A vulnerability was found in Funadmin up to 3.2.3. It has been declared as problematic. Affected by this vulnerability is the function tagLoad of the file Cx.php. The manipulation of the argument file leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB- 227869 was assigned to this vulnerability. <b>CVE ID : CVE-2023-</b> <b>2477</b>	N/A	A-FUN-FUNA- 170523/493

0-1

1-2

**2-3** 3-4 4-5 Page **259** of **1106**  5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Vendor: gen	ninilabs	•		L			
Product: sit	e_reviews						
Affected Ver	sion(s): * Up to (e	excluding)	6.7.1				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	4.8	The Site Reviews WordPress plugin before 6.7.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). <b>CVE ID : CVE-2023-</b> <b>1525</b>	N/A	A-GEM-SITE- 170523/494		
Vendor: gen	nomedics				<u> </u>		
Product: mi	llegpg						
Affected Ver	sion(s): 5.9.2						
Incorrect Permission Assignmen t for Critical Resource	04-May-2023	7.8	An issue was discovered in Genomedics MilleGP5 5.9.2, allows remote attackers to execute arbitrary code and gain escalated privileges via modifying specific files.	https://mille gpg.it/	A-GEN-MILL- 170523/495		
			CVE ID : CVE-2023- 25438				
Vendor: Geo	ovision			I			
Product: gv	Product: gv-edge_recording_manager						

0-1

1-2

2-33-44-5Page 260 of 1106

5-6

Affected Version(s): 2.2.3.0Incorrect Default Permission s04-May-20239.8An issue was discovered in GeoVision GV-Edge Recording Manager 2.2.3.0 for windows, which contains improper permissions within the default installation and allows attackers to execute arbitrary code and gain escalated privileges. CVE ID : CVE-2023- 23059N/AA-GEO-GV-E- 170523/496Vendor: getrebuildProduct: rebuildA vulnerability has been found in Rebuild 3.2 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery (CSRF)A-GET-REBU- 170523/49702-May-20234.3A vulnerability has been found in Rebuild 3.2 and classified as problematic. This vulnerability affects unknown code. 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. It is recommended to change the configuration settings. VDB- 227866 is the identifier assigned to this vulnerability.N/AA-GET-REBU- 170523/497	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Incorrect Default Permission s 4-May-2023 9-May-20	Affected Ver	Affected Version(s): 2.2.3.0							
Product: rebuildAffected Version(s): 3.2A vulnerability has been found in Rebuild 3.2 and classified as problematic. This vulnerability affects unknown code. 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. It is recommended to change the configuration settings. VDB- 227866 is the identifier assigned toN/AA-GET-REBU- 170523/497	Default Permission	04-May-2023	9.8	discovered in GeoVision GV-Edge Recording Manager 2.2.3.0 for windows, which contains improper permissions within the default installation and allows attackers to execute arbitrary code and gain escalated privileges.	N/A				
Affected Version(s): 3.2Cross-Site Request Forgery (CSRF)02-May-2023AA vulnerability has been found in Rebuild 3.2 and classified as problematic. This vulnerability affects unknown code. 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. It is recommended to change the configuration settings. VDB- 227866 is the identifier assigned toN/AA-GET-REBU- 170523/497	Vendor: ge	trebuild							
Cross-Site Request Forgery (CSRF)02-May-20234.3A vulnerability has been found in Rebuild 3.2 and classified as problematic. This vulnerability affects unknown code. 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. It is recommended to change the configuration settings. VDB- 227866 is the identifier assigned toN/AA-GET-REBU- 170523/497	Product: re	build							
Cross-Site Request Forgery (CSRF)02-May-20234.3been found in Rebuild 3.2 and classified as problematic. This vulnerability affects unknown code. 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. It is recommended to change the configuration settings. VDB- 227866 is the identifier assigned toN/AA-GET-REBU- 170523/497	Affected Ver	rsion(s): 3.2							
	Request Forgery	02-May-2023	4.3	been found in Rebuild 3.2 and classified as problematic. This vulnerability affects unknown code. 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. It is recommended to change the configuration settings. VDB- 227866 is the identifier assigned to	N/A				

2-3 Page **261** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 2474		
Vendor: gho	ost				
Product: gh	ost				
Affected Ver	sion(s): * Up to (e	excluding)	5.42.1		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-May-2023	7.5	Ghost before 5.42.1 allows remote attackers to read arbitrary files within the active theme's folder via /assets/built%2F% 2F%2F/ directory traversal. This occurs in frontend/web/middl eware/static- theme.js. <b>CVE ID : CVE-2023-</b>	https://githu b.com/TryG host/Ghost/ commit/378 dd913aa8d0 fd0da29b0ff ced8884579 598b0f	A-GHO-GHOS- 170523/498
Affected Ver	sion(s): * Up to (e	excluding	32235		
N/A	08-May-2023	7.5	Ghost is an app for new-media creators with tools to build a website, publish content, send newsletters, and offer paid subscriptions to members. Prior to version 5.46.1, due to a lack of validation when filtering on the public API endpoints, it is possible to reveal private fields via a brute force attack.	https://githu b.com/TryG host/Ghost/ security/adv isories/GHS A-r97q- ghch-82j9, https://githu b.com/TryG host/Ghost/ commit/b3c af16005289c c990948839 1b4a26f3f4a 66a90	A-GHO-GHOS- 170523/499
			Ghost(Pro) has already been		

0-1

1-2

2-33-44-5Page 262 of 1106

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID						
			patched. Maintainers can find no evidence that the issue was exploited on Ghost(Pro) prior to the patch being added. Self-hosters are impacted if running Ghost a version below v5.46.1. v5.46.1 contains a fix for this issue. As a workaround, add a block for requests to `/ghost/api/content /*` where the `filter` query parameter contains `password` or `email`. <b>CVE ID : CVE-2023-</b>								
			31133								
Vendor: gin	-gonic										
Product: gi											
Affected Ver	sion(s): * Up to (e	excluding)			I						
Improper Input Validation	04-May-2023	9.8	Versions of the package github.com/gin- gonic/gin before 1.9.0 are vulnerable to Improper Input Validation by allowing an attacker to use a specially crafted request via the X-Forwarded- Prefix header, potentially leading to cache poisoning. **Note:** Although this issue does not	https://githu b.com/t0rch wo0d/gin/c ommit/fd9f9 8e70fb4107 ee68c78348 2d231d35e6 0507b, https://githu b.com/gin- gonic/gin/p ull/3500, https://secu rity.snyk.io/ vuln/SNYK- GOLANG- GITHUBCOM	A-GIN-GIN- 170523/500						
CVSS Scoring	Scale 0-1	L-2 2-3	<b>3-4 4-5 5-6</b>	6-7 7-8	CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10						

Page 263 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			pose a significant threat on its own it can serve as an input vector for other more impactful vulnerabilities. However, successful exploitation may depend on the server configuration and whether the header is used in the application logic. <b>CVE ID : CVE-2023-</b>	GINGONICGI N-3324285, https://githu b.com/gin- gonic/gin/p ull/3503				
Vendor: Git	lah		26125					
Product: git								
	sion(s): * Up to (e	excluding)	15.8.5					
URL Redirectio n to Untrusted Site ('Open Redirect')	03-May-2023	5.4	An issue has been discovered in GitLab CE/EE affecting all versions before 15.8.5, 15.9.4, 15.10.1. Open redirects was possible due to framing arbitrary content on any page allowing user controlled markdown <b>CVE ID : CVE-2023-</b> <b>0155</b>	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 0155.json	A-GIT-GITL- 170523/501			
Affected Ver	Affected Version(s): * Up to (excluding) 15.9.6							
N/A	03-May-2023	8	An issue has been discovered in GitLab affecting all versions before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 0756.json	A-GIT-GITL- 170523/502			

0-1

1-2

**2-3** 3-4 4-5 Page **264** of **1106**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			starting from 15.11 before 15.11.1. The main branch of a repository with a specially crafted name allows an attacker to create repositories with malicious code, victims who clone or download these repositories will execute arbitrary code on their systems. <b>CVE ID : CVE-2023-</b>					
			0756					
Affected Ver	sion(s): 15.11.0				Γ			
N/A	03-May-2023	8.8	An issue has been discovered in GitLab EE affecting all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. Under certain conditions when OpenID Connect is enabled on an instance, it may allow users who are marked as 'external' to become 'regular' users thus leading to privilege escalation for those users. <b>CVE ID : CVE-2023-</b> <b>2182</b>	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 2182.json, https://gitla b.com/gitlab -org/gitlab/- /issues/403 012	A-GIT-GITL- 170523/503			
Affected Ver	Affected Version(s): From (including) 10.0 Up to (excluding) 12.9.8							
N/A	03-May-2023	4.3	An issue has been discovered in GitLab	https://gitla b.com/gitlab	A-GIT-GITL- 170523/504			
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5-6	6-7 7-8	<u> </u>			

Page 265 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affecting all versions starting from 10.0 before 12.9.8, all versions starting from 12.10 before 12.10.7, all versions starting from 13.0 before 13.0.1. A user could use an unverified email as a public email and commit email by sending a specifically crafted request on user update settings.	-org/cves/- /blob/maste r/2023/CVE -2023- 1204.json	
			CVE ID : CVE-2023- 1204		
Exposure of Resource to Wrong Sphere	03-May-2023	4.3	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 12.9.8, all versions starting from 12.10 before 12.10.7, all versions starting from 13.0 before 13.0.1. A user with the role of developer could use the import project feature to leak CI/CD variables. <b>CVE ID : CVE-2023- 2069</b>	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 2069.json	A-GIT-GITL- 170523/505
Affected Ver	<mark>sion(s): From (in</mark>	cluding) 1	1.9 Up to (excluding) 1	5.9.6	
Session Fixation	03-May-2023	4.5	An issue has been discovered in GitLab affecting all versions starting from 11.9 before 15.9.6, all versions starting from 15.10 before	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 1265.json	A-GIT-GITL- 170523/506

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.10.5, all versions starting from 15.11 before 15.11.1. The condition allows for a privileged attacker, under certain conditions, to obtain session tokens from all users of a GitLab instance. <b>CVE ID : CVE-2023-</b> <b>1265</b>		
Affected Ver	sion(s): From (in	cluding) 1	2.10 Up to (excluding)	12.10.7	
N/A	03-May-2023	4.3	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 12.9.8, all versions starting from 12.10 before 12.10.7, all versions starting from 13.0 before 13.0.1. A user could use an unverified email as a public email and commit email by sending a specifically crafted request on user update settings. <b>CVE ID : CVE-2023-</b> <b>1204</b>	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 1204.json	A-GIT-GITL- 170523/507
Affected Ver	sion(s): From (in	cluding) 1	2.10.0 Up to (excluding	) 12.10.7	
Exposure of Resource to Wrong Sphere	03-May-2023	4.3	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 12.9.8, all versions starting from 12.10 before 12.10.7, all versions starting from 13.0	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 2069.json	A-GIT-GITL- 170523/508

0-1

1-2

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 13.0.1. A user with the role of developer could use the import project feature to leak CI/CD variables. <b>CVE ID : CVE-2023-</b> <b>2069</b>		
Affected Ver	sion(s): From (in	cluding) 1	3.0 Up to (excluding) 1	3.0.1	
N/A	03-May-2023	4.3	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 12.9.8, all versions starting from 12.10 before 12.10.7, all versions starting from 13.0 before 13.0.1. A user could use an unverified email as a public email and commit email by sending a specifically crafted request on user update settings. <b>CVE ID : CVE-2023-</b> <b>1204</b>	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 1204.json	A-GIT-GITL- 170523/509
Exposure of Resource to Wrong Sphere	03-May-2023	4.3	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 12.9.8, all versions starting from 12.10 before 12.10.7, all versions starting from 13.0 before 13.0.1. A user with the role of developer could use the import project	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 2069.json	A-GIT-GITL- 170523/510

0-1

1-2

7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			feature to leak CI/CD variables.		
			CVE ID : CVE-2023- 2069		
Affected Ver	sion(s): From (in	cluding) 1	3.11 Up to (excluding)	15.8.5	
Exposure of Resource to Wrong Sphere	03-May-2023	6.5	An issue has been discovered in GitLab affecting all versions starting from 13.11 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. It was possible that a project member demoted to a user role to read project updates by doing a diff with a pre- existing fork. <b>CVE ID : CVE-2023- 0485</b>	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 0485.json	A-GIT-GITL- 170523/511
Affected Ver	<mark>sion(s): From (in</mark>	cluding) 1	4.2 Up to (excluding) 1	5.9.6	
Cross-Site Request Forgery (CSRF)	03-May-2023	6.5	An issue has been discovered in GitLab EE affecting all versions starting from 14.2 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. Lack of verification on RelayState parameter allowed a maliciously crafted URL to obtain access tokens granted for	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 1965.json	A-GIT-GITL- 170523/512

0-1

1-2

**2-3** 3-4 4-5 Page **269** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3rd party Group SAML SSO logins. This feature isn't enabled by default. CVE ID : CVE-2023- 1965		
Affected Vers	sion(s): From (in	cluding) 1	5.10 Up to (excluding)	15.10.1	1
URL Redirectio n to Untrusted Site ('Open Redirect')	03-May-2023	5.4	An issue has been discovered in GitLab CE/EE affecting all versions before 15.8.5, 15.9.4, 15.10.1. Open redirects was possible due to framing arbitrary content on any page allowing user controlled markdown <b>CVE ID : CVE-2023-</b> <b>0155</b>	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 0155.json	A-GIT-GITL- 170523/513
Affected Vers	sion(s): From (in	cluding) 1	5.10 Up to (excluding)	15.10.5	
N/A	03-May-2023	8.1	An issue has been discovered in GitLab EE affecting all versions starting from 15.2 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. A malicious group member may continue to have access to the public projects of a public group even after being banned from the public group by the owner.	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 0805.json	A-GIT-GITL- 170523/514
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4 4-5 5-6	6-7 7-8	<u> </u>

Page 270 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 0805		
N/A	03-May-2023	8	An issue has been discovered in GitLab affecting all versions before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. The main branch of a repository with a specially crafted name allows an attacker to create repositories with malicious code, victims who clone or download these repositories will execute arbitrary code on their systems. <b>CVE ID : CVE-2023- 0756</b>	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 0756.json	A-GIT-GITL- 170523/515
Cross-Site Request Forgery (CSRF)	03-May-2023	6.5	An issue has been discovered in GitLab EE affecting all versions starting from 14.2 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. Lack of verification on RelayState parameter allowed a maliciously crafted URL to obtain access tokens granted for	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 1965.json	A-GIT-GITL- 170523/516

0-1

1-2

2-33-44-5Page 271 of 1106

5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3rd party Group SAML SSO logins. This feature isn't enabled by default. <b>CVE ID : CVE-2023-</b>		
Improper Control of Generation of Code ('Code Injection')	03-May-2023	5.7	1965An issue has been discovered in GitLab CE/EE affecting all versions from 8.6 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. File integrity may be compromised when source code or installation packages are pulled from a tag or from a release containing a ref to another commit.CVE ID : CVE-2023- 1178	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 1178.json	A-GIT-GITL- 170523/517
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	5.4	A cross-site scripting issue has been discovered in GitLab affecting all versions starting from 5.1 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. When viewing an XML file in a repository in "raw" mode, it can be made to render as HTML if viewed	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 1836.json	A-GIT-GITL- 170523/518

0-1

1-2

2-33-44-5Page 272 of 1106

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			under specific circumstances <b>CVE ID : CVE-2023-</b>		
Session Fixation	03-May-2023	4.5	1836 An issue has been discovered in GitLab affecting all versions starting from 11.9 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. The condition allows for a privileged attacker, under certain conditions, to obtain session tokens from all users of a GitLab instance. <b>CVE ID : CVE-2023-</b> 1265	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 1265.json	A-GIT-GITL- 170523/519
Affected Ver	sion(s): From (in	cluding) 1	5.10.0 Up to (excluding	) 15.10.5	
N/A	03-May-2023	8.8	An issue has been discovered in GitLab EE affecting all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. Under certain conditions when OpenID Connect is enabled on an instance, it may allow users who are marked as 'external' to become 'regular' users thus leading to	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 2182.json, https://gitla b.com/gitlab -org/gitlab/- /issues/403 012	A-GIT-GITL- 170523/520

0-1

1-2

2-33-44-5Page 273 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege escalation for those users. CVE ID : CVE-2023- 2182		
Affected Ver	sion(s): From (in	cluding) 1	5.10.0 Up to (excluding	) 15.10.6	
Incorrect Permission Assignmen t for Critical Resource	08-May-2023	6.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 before 15.9.7, all versions starting from 15.10 before 15.10.6, all versions starting from 15.11 before 15.11.2. Under certain conditions, a malicious unauthorized GitLab user may use a GraphQL endpoint to attach a malicious runner to any project. <b>CVE ID : CVE-2023-</b> <b>2478</b>	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 2478.json	A-GIT-GITL- 170523/521
Affected Ver	sion(s): From (in	cluding) 1	5.11 Up to (excluding)	15.11.1	
N/A	03-May-2023	8.1	An issue has been discovered in GitLab EE affecting all versions starting from 15.2 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. A malicious group member may continue to have access to the public projects of a public	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 0805.json	A-GIT-GITL- 170523/522

0-1

1-2

**2-3** 3-4 4-5 Page **274** of **1106**  5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			group even after being banned from the public group by the owner. <b>CVE ID : CVE-2023-</b> <b>0805</b>		
N/A	03-May-2023	8	An issue has been discovered in GitLab affecting all versions before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. The main branch of a repository with a specially crafted name allows an attacker to create repositories with malicious code, victims who clone or download these repositories will execute arbitrary code on their systems. <b>CVE ID : CVE-2023- 0756</b>	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 0756.json	A-GIT-GITL- 170523/523
Exposure of Resource to Wrong Sphere	03-May-2023	6.5	An issue has been discovered in GitLab affecting all versions starting from 13.11 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. It was possible that a project member demoted to a user	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 0485.json	A-GIT-GITL- 170523/524

0-1

1-2

2-33-44-5Page 275 of 1106

7-8

6-7

5-6

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			role to read project updates by doing a diff with a pre- existing fork. <b>CVE ID : CVE-2023-</b>		
Cross-Site Request Forgery (CSRF)	03-May-2023	6.5	0485 An issue has been discovered in GitLab EE affecting all versions starting from 14.2 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. Lack of verification on RelayState parameter allowed a maliciously crafted URL to obtain access tokens granted for 3rd party Group SAML SSO logins. This feature isn't enabled by default. <b>CVE ID : CVE-2023- 1965</b>	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 1965.json	A-GIT-GITL- 170523/525
Improper Control of Generation of Code ('Code Injection')	03-May-2023	5.7	An issue has been discovered in GitLab CE/EE affecting all versions from 8.6 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. File integrity may be compromised when source code or installation packages	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 1178.json	A-GIT-GITL- 170523/526

0-1

1-2

2-33-44-5Page 276 of 1106

7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are pulled from a tag or from a release containing a ref to another commit.		
			CVE ID : CVE-2023- 1178		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	5.4	A cross-site scripting issue has been discovered in GitLab affecting all versions starting from 5.1 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. When viewing an XML file in a repository in "raw" mode, it can be made to render as HTML if viewed under specific circumstances <b>CVE ID : CVE-2023-</b> <b>1836</b>	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 1836.json	A-GIT-GITL- 170523/527
Session Fixation	03-May-2023	4.5	An issue has been discovered in GitLab affecting all versions starting from 11.9 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. The condition allows for a privileged attacker, under certain conditions, to obtain session tokens from	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 1265.json	A-GIT-GITL- 170523/528

0-1

1-2

2-33-44-5Page 277 of 1106

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all users of a GitLab instance. CVE ID : CVE-2023- 1265		
Affected Ver	sion(s): From (in	cluding) 1	5.11.0 Up to (excluding	) 15.11.2	
Incorrect Permission Assignmen t for Critical Resource	08-May-2023	6.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 before 15.9.7, all versions starting from 15.10 before 15.10.6, all versions starting from 15.11 before 15.11.2. Under certain conditions, a malicious unauthorized GitLab user may use a GraphQL endpoint to attach a malicious runner to any project. <b>CVE ID : CVE-2023-</b> <b>2478</b>	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 2478.json	A-GIT-GITL- 170523/529
Affected Ver	sion(s): From (in	cluding) 1	5.2 Up to (excluding) 1	5.9.6	
N/A	03-May-2023	8.1	An issue has been discovered in GitLab EE affecting all versions starting from 15.2 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. A malicious group member may continue to have access to the public projects of a public	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 0805.json	A-GIT-GITL- 170523/530

0-1

1-2

**2-3** 3-4 4-5 Page **278** of **1106**  5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			group even after being banned from the public group by the owner.		
			CVE ID : CVE-2023- 0805		
Affected Ver	sion(s): From (in	cluding) 1	5.4.0 Up to (excluding)	15.9.7	-
Incorrect Permission Assignmen t for Critical Resource	08-May-2023	6.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 before 15.9.7, all versions starting from 15.10 before 15.10.6, all versions starting from 15.11 before 15.11.2. Under certain conditions, a malicious unauthorized GitLab user may use a GraphQL endpoint to attach a malicious runner to any project. <b>CVE ID : CVE-2023-</b> 2478	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 2478.json	A-GIT-GITL- 170523/531
Affected Ver	sion(s): From (in	cluding) 1	5.9 Up to (excluding) 1	5.9.4	
Exposure of Resource to Wrong Sphere	03-May-2023	6.5	An issue has been discovered in GitLab affecting all versions starting from 13.11 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. It was possible that a project member demoted to a user	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 0485.json	A-GIT-GITL- 170523/532

0-1

1-2

**2-3** 3-4 4-5 Page **279** of **1106**  5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			role to read project updates by doing a diff with a pre- existing fork.		
			CVE ID : CVE-2023- 0485		
Affected Ver	<mark>sion(s): From (in</mark>	cluding) 1	5.9 Up to (excluding) 1	5.9.5	1
URL Redirectio n to Untrusted Site ('Open Redirect')	03-May-2023	5.4	An issue has been discovered in GitLab CE/EE affecting all versions before 15.8.5, 15.9.4, 15.10.1. Open redirects was possible due to framing arbitrary content on any page allowing user controlled markdown	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 0155.json	A-GIT-GITL- 170523/533
			CVE ID : CVE-2023- 0155		
Affected Ver	sion(s): From (in	cluding) 5	.1 Up to (excluding) 15. A cross-site scripting	9.6	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	5.4	issue has been discovered in GitLab affecting all versions starting from 5.1 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. When viewing an XML file in a repository in "raw" mode, it can be made to render as HTML if viewed under specific circumstances	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 1836.json	A-GIT-GITL- 170523/534

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2023- 1836					
Affected Ver	sion(s): From (in	cluding) 8	.6.0 Up to (excluding) 1	5.9.6	·			
Improper Control of Generation of Code ('Code Injection')	03-May-2023	5.7	An issue has been discovered in GitLab CE/EE affecting all versions from 8.6 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. File integrity may be compromised when source code or installation packages are pulled from a tag or from a release containing a ref to another commit. <b>CVE ID : CVE-2023-</b> <b>1178</b>	https://gitla b.com/gitlab -org/cves/- /blob/maste r/2023/CVE -2023- 1178.json	A-GIT-GITL- 170523/535			
Vendor: giv	ewp			1				
Product: giv	/ewp							
Affected Ver	sion(s): * Up to (e	excluding)	2.25.2					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in GiveWP plugin <= 2.25.1 versions. CVE ID : CVE-2023- 23668	N/A	A-GIV-GIVE- 170523/536			
Vendor: gm	0							
Product: typesquare_webfonts_for_conoha								
Affected Version(s): * Up to (excluding) 2.0.4								
Improper Neutralizat	04-May-2023	4.8	Auth. (admin+) Stored Cross-Site	N/A	A-GMO-TYPE- 170523/537			
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4 4-5 5-	6 6-7 7-6	8 8-9 <mark>9-10</mark>			

				NCIIPC ID
		Scripting (XSS) vulnerability in GMO Internet Group, Inc. TypeSquare Webfonts for ConoHa plugin <= 2.0.3 versions. CVE ID : CVE-2023- 25458		
ogle		20100		
rome				
sion(s): * Up to (e	excluding)	113.0.5672.63		
03-May-2023	8.8	Use after free in OS Inputs in Google Chrome on ChromeOS prior to 113.0.5672.63 allowed a remote attacker who convinced a user to enage in specific UI interaction to potentially exploit heap corruption via crafted UI interaction. (Chromium security severity: Medium) <b>CVE ID : CVE-2023- 2461</b>	N/A	A-GOO-CHRO- 170523/538
03-May-2023	7.1	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to bypass file access checks via a crafted	N/A	A-GOO-CHRO- 170523/539
	rome sion(s): * Up to (e	rome sion(s): * Up to (excluding) 03-May-2023 8.8	vulnerability in GMO Internet Group, Inc. TypeSquare Webfonts for ConoHa plugin <= 2.0.3 versions.cypeCype Square Webfonts for ConoHa plugin <= 2.0.3 versions.cype SogleromeUse after free in OS Inputs in Google Chrome on ChromeOS prior to 113.0.5672.63 allowed a remote attacker who convinced a user to enage in specific UI interaction to potentially exploit heap corruption via crafted UI interaction. (Chromium security severity: Medium)03-May-20238.8Insufficient validation of untrusted input in Extensions in Google Chrome prior to 113.0.5672.63 allowed a remote attacker who convinced a user to enage in specific UI interaction. (Chromium security severity: Medium)03-May-20237.1Insufficient validation of untrusted input in Extensions in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to bypass file access	vulnerability in GMO Internet Group, Inc. TypeSquare Webfonts for ConoHa plugin <= 2.0.3 versions.cysel

Page 282 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTML page. (Chromium security severity: Medium)		
			CVE ID : CVE-2023- 2460		
N/A	03-May-2023	6.5	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to bypass permission restrictions via a crafted HTML page. (Chromium security severity: Medium)	N/A	A-GOO-CHRO- 170523/540
			CVE ID : CVE-2023- 2459		
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to obfuscate main origin data via a crafted HTML page. (Chromium security severity: Medium) <b>CVE ID : CVE-2023-</b> 2462	N/A	A-GOO-CHRO- 170523/541
N/A	03-May-2023	4.3	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to hide the contents of the Omnibox (URL bar)	N/A	A-GOO-CHRO- 170523/542

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via a crafted HTML page. (Chromium security severity: Medium) <b>CVE ID : CVE-2023-</b>		
N/A	03-May-2023	4.3	2463 Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to perform an origin spoof in the security UI via a crafted HTML page. (Chromium security severity: Medium) CVE ID : CVE-2023- 2464	N/A	A-GOO-CHRO- 170523/543
N/A	03-May-2023	4.3	Inappropriate implementation in CORS in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) <b>CVE ID : CVE-2023-</b> <b>2465</b>	N/A	A-GOO-CHRO- 170523/544
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote	N/A	A-GOO-CHRO- 170523/545

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to spoof the contents of the security UI via a crafted HTML page. (Chromium security severity: Low)		
			CVE ID : CVE-2023- 2466		
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to bypass permissions restrictions via a crafted HTML page. (Chromium security severity: Low) <b>CVE ID : CVE-2023-</b>	N/A	A-GOO-CHRO- 170523/546
N/A	03-May-2023	4.3	2467 Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed a remote attacker who had compromised the renderer process to obfuscate the security UI via a crafted HTML page. (Chromium security severity: Low) CVE ID : CVE-2023- 2468	N/A	A-GOO-CHRO- 170523/547
Product: we	b_stories		<u></u>		
Affected Ver	sion(s): * Up to (e	excluding)	1.32.0		

0-1

1-2

**2-3** 3-4 4-5 Page **285** of **1106**  5-6

6-7

8-9

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorizati on	08-May-2023	6.5	The Web Stories for WordPress plugin supports the WordPress built-in functionality of protecting content with a password. The content is then only accessible to website visitors after entering the password. In WordPress, users with the "Author" role can create stories, but don't have the ability to edit password protected stories. The vulnerability allowed users with said role to bypass this permission check when trying to duplicate the protected story in the plugin's own dashboard, giving them access to the seemingly protected content. We recommend upgrading to version 1.32 or beyond commit ad49781c2a 35c5c92ef704d4b62 1ab4e5cb77d68 https://github.com/ GoogleForCreators/ web-stories- wp/commit/ad4978 1c2a35c5c92ef704d	https://githu b.com/Googl eForCreators /web- stories- wp/commit/ ad49781c2a 35c5c92ef70 4d4b621ab4 e5cb77d68	A-GOO-WEB 170523/548

0-1

1-2

**2-3** 3-4 4-5 Page **286** of **1106**  5-6

7-8

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 1979		
Vendor: gre	entreelabs				
Product: cir	cles_gallery				
Affected Vers	sion(s): * Up to (i	ncluding)	1.0.10		
Improper Neutralizat ion of Input During Web Page Generation	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in GreenTreeLabs Circles Gallery plugin <= 1.0.10 versions.	N/A	A-GRE-CIRC- 170523/549
('Cross-site Scripting')			CVE ID : CVE-2023- 23881		
Vendor: has	shicorp				
Product: va	ult				
Affected Ver	sion(s): From (in	cluding) 1	.13.0 Up to (excluding)	1.13.2	
Inadequate Encryption Strength	01-May-2023	2.5	HashiCorp Vault Enterprise 1.13.0 up to 1.13.1 is vulnerable to a padding oracle attack when using an HSM in conjunction with the CKM_AES_CBC_P AD or CKM_AES_CBC encryption mechanisms. An attacker with privileges to modify storage and restart Vault may be able to intercept or modify cipher text in order to derive Vault's root key. Fixed in 1.13.2 <b>CVE ID : CVE-2023-</b> <b>2197</b>	https://disc uss.hashicor p.com/t/hcs ec-2023-14- vault- enterprise- vulnerable- to-padding- oracle- attacks- when-using- a-cbc-based- encryption- mechanism- with-a- hsm/53322	A-HAS-VAUL- 170523/550

0-1

1-2

**2-3** 3-4 4-5 Page **287** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: hu-	manity				I
Product: co	okie_notice_\&_	complian	ce_for_gdpr_\/_ccpa		
Affected Ver	sion(s): * Up to (e	excluding)	2.4.7		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	07-May-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Hu-manity.Co Cookie Notice & Compliance for GDPR / CCPA plugin <= 2.4.6 versions. <b>CVE ID : CVE-2023-</b> 24400	N/A	A-HUCOOK- 170523/551
Vendor: IBN	1				1
Product: bu	siness_automat	ion_work	flow		
Affected Ver	sion(s): 18.0.0.0				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 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: 246115. <b>CVE ID : CVE-2023- 24957</b>	https://ww w.ibm.com/s upport/page s/node/696 5776, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24611 5	A-IBM-BUSI- 170523/552

0-1

1-2

**2-3** 3-4 4-5 Page **288** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 18.0.0.1	I			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business         Automation         Workflow 18.0.0.0,         18.0.0.1, 18.0.2,         19.0.0.1, 19.0.2,         19.0.0.3, 20.0.1,         20.0.2, 21.0.2,         21.0.3, 22.0.1, and         22.0.2 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: 246115.	https://ww w.ibm.com/s upport/page s/node/696 5776, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24611 5	A-IBM-BUSI- 170523/553
Affected Von	$r_{1}$		24957		
Affected Ver	sion(s): 18.0.0.2		IBM Business		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the	https://ww w.ibm.com/s upport/page s/node/696 5776, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24611 5	A-IBM-BUSI- 170523/554

0-1

1-2

**2-3** 3-4 4-5 Page **289** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 246115.		
			CVE ID : CVE-2023- 24957		
Affected Ver	sion(s): 20.0.0.1				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 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: 246115. <b>CVE ID : CVE-2023- 24957</b>	https://ww w.ibm.com/s upport/page s/node/696 5776, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24611 5	A-IBM-BUSI- 170523/555
Affected Ver	sion(s): 20.0.0.2				
Improper Neutralizat ion of Input During Web Page	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1,	https://ww w.ibm.com/s upport/page s/node/696 5776, https://exch	A-IBM-BUSI- 170523/556

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 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: 246115.	ange.xforce.i bmcloud.co m/vulnerabi lities/24611 5	
			CVE ID : CVE-2023- 24957		
Affected Ver	sion(s): 21.0.3				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 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: 246115.	https://ww w.ibm.com/s upport/page s/node/696 5776, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24611 5	A-IBM-BUSI- 170523/557

0-1

1-2

2-33-44-5Page 291 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24957		
Affected Ver	sion(s): 22.0.1				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 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: 246115. <b>CVE ID : CVE-2023-</b> 24957	https://ww w.ibm.com/s upport/page s/node/696 5776, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24611 5	A-IBM-BUSI- 170523/558
Affected Ver	sion(s): 22.0.2			L	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed	https://ww w.ibm.com/s upport/page s/node/696 5776, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24611 5	A-IBM-BUSI- 170523/559

0-1

1-2

2-33-44-5Page 292 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			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: 246115. <b>CVE ID : CVE-2023-</b>					
			24957					
Affected Ver	sion(s): From (in	cluding) 1	9.0.0.1 Up to (including	) 19.0.0.3				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 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: 246115. <b>CVE ID : CVE-2023-</b> 24957	https://ww w.ibm.com/s upport/page s/node/696 5776, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24611 5	A-IBM-BUSI- 170523/560			
	Affected Version(s): From (including) 20.0.0.1 Up to (excluding) 21.0.3							
Improper Neutralizat ion of	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0,	https://ww w.ibm.com/s upport/page	A-IBM-BUSI- 170523/561			

0-1

1-2

2-33-44-5Page 293 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 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: 246115. <b>CVE ID : CVE-2023-</b> 24957	s/node/696 5776, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24611 5	
Affected Ver	sion(s): From (in	cluding) 2	24957 1.0.1 Up to (including)	21.0.3.1	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 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://ww w.ibm.com/s upport/page s/node/696 5776, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24611 5	A-IBM-BUSI- 170523/562

0-1

1-2

**2-3** 3-4 4-5 Page **294** of **1106**  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: 246115.		
			CVE ID : CVE-2023- 24957		
Affected Ver	<mark>sion(s): From (in</mark>	cluding) 2	2.0.1 Up to (excluding)	22.0.2	1
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 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: 246115. <b>CVE ID : CVE-2023-</b>	https://ww w.ibm.com/s upport/page s/node/696 5776, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24611 5	A-IBM-BUSI- 170523/563
			24957		
Product: clo					
Affected Ver	<mark>sion(s): * Up to (i</mark>	ncluding)	<b></b>		
N/A	02-May-2023	5.3	Design documents with matching document IDs, from databases on the same cluster, may share a mutable Javascript environment when	https://docs. couchdb.org /en/stable/c ve/2023- 26268.html	A-IBM-CLOU- 170523/564

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using these design document functions:		
			validate_doc_update		
			* list		
			* filter		
			* filter views (using view functions as filters)		
			* rewrite		
			* update		
			This doesn't affect map/reduce or search (Dreyfus) index functions.		
			Users are recommended to upgrade to a version that is no longer affected by this issue (Apache CouchDB 3.3.2 or 3.2.3).		
			Workaround: Avoid using design documents from untrusted sources which may attempt to cache or store		

0-1

1-2

**2-3** 3-4 4-5 Page **296** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data in the Javascript environment.		
			CVE ID : CVE-2023- 26268		
Product: ela	astic_storage_sys	stem			
Affected Ver	sion(s): From (in	cluding) 6	.1.0.0 Up to (excluding)	6.1.2.6	
Improper Input Validation	05-May-2023	5.5	IBM Storage Scale (IBM Spectrum Scale 5.1.0.0 through 5.1.2.9, 5.1.3.0 through 5.1.6.1 and IBM Elastic Storage Systems 6.1.0.0 through 6.1.2.5, 6.1.3.0 through 6.1.6.0) could allow a local user to cause a kernel panic. IBM X- Force ID: 252187. <b>CVE ID : CVE-2023-</b> <b>30434</b>	https://ww w.ibm.com/s upport/page s/node/698 8365, https://ww w.ibm.com/s upport/page s/node/698 8363, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/25218 7	A-IBM-ELAS- 170523/565
Affected Ver	sion(s): From (in	cluding) 6	.1.3.0 Up to (excluding)	6.1.6.1	
Improper Input Validation	05-May-2023	5.5	IBM Storage Scale (IBM Spectrum Scale 5.1.0.0 through 5.1.2.9, 5.1.3.0 through 5.1.6.1 and IBM Elastic Storage Systems 6.1.0.0 through 6.1.2.5, 6.1.3.0 through 6.1.6.0) could allow a local user to cause a kernel panic. IBM X- Force ID: 252187. <b>CVE ID : CVE-2023-</b> <b>30434</b>	https://ww w.ibm.com/s upport/page s/node/698 8365, https://ww w.ibm.com/s upport/page s/node/698 8363, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/25218 7	A-IBM-ELAS- 170523/566

0-1

1-2

**2-3** 3-4 4-5 Page **297** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Product: mo	1_appliance			I				
Affected Vers	sion(s): From (in	cluding) 9	.2.0.0 Up to (excluding)	9.2.0.11				
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-May-2023	7.5	IBM MQ 9.2 CD, 9.2 LTS, 9.3 CD, and 9.3 LTS could allow a remote attacker to cause a denial of service due to an error processing invalid data. IBM X- Force ID: 248418. <b>CVE ID : CVE-2023-</b> <b>26285</b>	https://ww w.ibm.com/s upport/page s/node/698 6563, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24841 8	A-IBM-MQ_A- 170523/567			
Affected Vers	sion(s): From (in	cluding) 9	.2.0.0 Up to (excluding)	9.2.5.7				
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-May-2023	7.5	IBM MQ 9.2 CD, 9.2 LTS, 9.3 CD, and 9.3 LTS could allow a remote attacker to cause a denial of service due to an error processing invalid data. IBM X- Force ID: 248418. <b>CVE ID : CVE-2023-</b> 26285	https://ww w.ibm.com/s upport/page s/node/698 6563, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24841 8	A-IBM-MQ_A- 170523/568			
Affected Vers	sion(s): From (in	cluding) 9	.2.0.0 Up to (excluding)	9.3.2				
Uncontroll ed Resource Consumpti on	05-May-2023	5.5	IBM MQ Clients 9.2 CD, 9.3 CD, and 9.3 LTS are vulnerable to a denial of service attack when processing configuration files. IBM X-Force ID: 244216. <b>CVE ID : CVE-2023- 22874</b>	https://ww w.ibm.com/s upport/page s/node/698 5901, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24421 6	A-IBM-MQ_A- 170523/569			
Affected Vers	Affected Version(s): From (including) 9.3.0.0 Up to (excluding) 9.3.0.5							
Improper Restriction	05-May-2023	7.5	IBM MQ 9.2 CD, 9.2 LTS, 9.3 CD, and 9.3	https://ww w.ibm.com/s	A-IBM-MQ_A- 170523/570			

CVSS Scoring Scale 0-1 1-2

**2-3** 3-4 4-5 Page **298** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			LTS could allow a remote attacker to cause a denial of service due to an error processing invalid data. IBM X- Force ID: 248418. <b>CVE ID : CVE-2023-</b> 26285	upport/page s/node/698 6563, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24841 8	
Uncontroll ed Resource Consumpti on	05-May-2023	5.5	IBM MQ Clients 9.2 CD, 9.3 CD, and 9.3 LTS are vulnerable to a denial of service attack when processing configuration files. IBM X-Force ID: 244216. <b>CVE ID : CVE-2023- 22874</b>	https://ww w.ibm.com/s upport/page s/node/698 5901, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24421 6	A-IBM-MQ_A- 170523/571
Affected Ver	sion(s): From (in	cluding) 9	.3.0.0 Up to (excluding)	9.3.2.1	
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-May-2023	7.5	IBM MQ 9.2 CD, 9.2 LTS, 9.3 CD, and 9.3 LTS could allow a remote attacker to cause a denial of service due to an error processing invalid data. IBM X- Force ID: 248418. <b>CVE ID : CVE-2023-</b> <b>26285</b>	https://ww w.ibm.com/s upport/page s/node/698 6563, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24841 8	A-IBM-MQ_A- 170523/572
	ectrum_scale	1 11 2 -		5120	
Attected Ver	sion(s): From (in	cluding) 5	.1.0.0 Up to (including)	1	
Improper Input Validation	05-May-2023	5.5	IBM Storage Scale (IBM Spectrum Scale 5.1.0.0 through 5.1.2.9, 5.1.3.0 through 5.1.6.1 and IBM Elastic Storage Systems 6.1.0.0	https://ww w.ibm.com/s upport/page s/node/698 8365, https://ww w.ibm.com/s	A-IBM-SPEC- 170523/573

 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
			through 6.1.2.5, 6.1.3.0 through 6.1.6.0) could allow a local user to cause a kernel panic. IBM X- Force ID: 252187. <b>CVE ID : CVE-2023-</b> <b>30434</b>	upport/page s/node/698 8363, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/25218 7	
Affected Ver	sion(s): From (in	cluding) 5	.1.3.0 Up to (including)		I
Improper Input Validation	05-May-2023	5.5	IBM Storage Scale (IBM Spectrum Scale 5.1.0.0 through 5.1.2.9, 5.1.3.0 through 5.1.6.1 and IBM Elastic Storage Systems 6.1.0.0 through 6.1.2.5, 6.1.3.0 through 6.1.6.0) could allow a local user to cause a kernel panic. IBM X- Force ID: 252187. <b>CVE ID : CVE-2023-</b> <b>30434</b>	https://ww w.ibm.com/s upport/page s/node/698 8365, https://ww w.ibm.com/s upport/page s/node/698 8363, https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/25218 7	A-IBM-SPEC- 170523/574
Vendor: Illu	imos				
Product: ill	umos-gate				
Affected Ver	sion(s): * Up to (e	excluding)	2023-04-29		
Out-of- bounds Write	04-May-2023	7.8	illumos illumos-gate before 676abcb has a stack buffer overflow in /dev/net, leading to privilege escalation via a stat on a long file name in /dev/net. <b>CVE ID : CVE-2023-</b> <b>31284</b>	N/A	A-ILL-ILLU- 170523/575
Vendor: ipa	ndao				
Product: ed	itor.md				
0.452.2					
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>300</b> of <b>1106</b>	6-7 7-8	3 8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): * Up to (i	ncluding)	1.5.0		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	01-May-2023	6.1	Cross Site Scripting (XSS) vulnerability in pandao editor.md thru 1.5.0 allows attackers to inject arbitrary web script or HTML via crafted markdown text. CVE ID : CVE-2023- 29641	https://githu b.com/pand ao/editor.m d/issues/98 5	A-IPA-EDIT- 170523/576
Vendor: j2e	efast				I
Product: j2e	eefast				
Affected Ver	sion(s): * Up to (i	ncluding)	2.6.0		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	5.4	A vulnerability was found in Dromara J2eeFAST up to 2.6.0 and classified as problematic. This issue affects some unknown processing of the component System Message Handler. The manipulation of the argument ?? leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 7a9e1a00e3329fdc0 ae05f7a8257cce770 37134d. It is recommended to apply a patch to fix this issue. The associated identifier	N/A	A-J2E-J2EE- 170523/577

0-1

1-2

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	of this vulnerability is VDB-227867. <b>CVE ID : CVE-2023- 2475</b> A vulnerability was found in Dromara J2eeFAST up to 2.6.0. It has been classified as problematic. Affected is an unknown function of the component Announcement Handler. The manipulation of the argument ????/??? leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be	Patch	NCIIPC ID
('Cross-site Scripting')			used. The name of the patch is 7a9e1a00e3329fdc0 ae05f7a8257cce770 37134d. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB- 227868. <b>CVE ID : CVE-2023-</b> 2476		
Vendor: jch	_optimize_proje	ct			
Product: jch	_optimize				
Affected Vers	sion(s): * Up to (e	excluding)	<b></b>		
Improper Neutralizat ion of	06-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS)	N/A	A-JCH-JCH 170523/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			vulnerability in Samuel Marshall JCH Optimize plugin <= 3.2.2 versions. CVE ID : CVE-2023- 25491		
Vendor: jsre	enort		23471		
Product: jsr	-				
-	sion(s): * Up to (e	excluding)	) 3.11.3		
Improper Control of Generation of Code ('Code Injection')	08-May-2023	10	Code Injection in GitHub repository jsreport/jsreport prior to 3.11.3. <b>CVE ID : CVE-2023- 2583</b>	https://githu b.com/jsrep ort/jsreport /commit/afa ff3804b34b3 8e959f5ae65 f9e672088d e13d7, https://hunt r.dev/bounti es/397ea68 d-1e28-44ff- b830- c8883d067d 96	A-JSR-JSRE- 170523/580
Vendor: jud	ging_manageme	ent_syste	m_project		
Product: juo	lging_managem	ent_syste	em		
Affected Ver	sion(s): 1.0				1
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	08-May-2023	9.8	Judging Management System v1.0 is vulnerable to SQL Injection. via /php- jms/review_se_result .php?mainevent_id=. CVE ID : CVE-2023- 30018	N/A	A-JUD-JUDG- 170523/581
Improper Neutralizat ion of	04-May-2023	9.8	Judging Management System v1.0 by oretnom23 was	N/A	A-JUD-JUDG- 170523/582

CVSS Scoring Scale0-11-22-3

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			discovered to vulnerable to SQL injection via /php- jms/review_result.ph p?mainevent_id=, mainevent_id. CVE ID : CVE-2023- 30077		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	04-May-2023	9.8	Judging Management System v1.0 was discovered to contain a SQL injection vulnerability via the event_id parameter at /php- jms/result_sheet.php CVE ID : CVE-2023- 30203	N/A	A-JUD-JUDG- 170523/583
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	03-May-2023	9.8	Judging Management System v1.0 was discovered to contain a SQL injection vulnerability via the judge_id parameter at /php- jms/edit_judge.php. <b>CVE ID : CVE-2023-</b> <b>30204</b>	N/A	A-JUD-JUDG- 170523/584
Vendor: kan					
	nban_boards_fo				
Improper Neutralizat ion of Input During Web Page Generation	09-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kanban for WordPress Kanban Boards for	N/A	A-KAN-KANB- 170523/585
CVSS Scoring S	icale 0-1 1	-2 2-3	<b>3-4 4-5 5-6</b>	6-7 7-8	<u>8 8-9 9-10</u>

Page **304** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			WordPress plugin <= 2.5.20 versions. CVE ID : CVE-2023- 23884		
Vendor: kor	ıga_project				1
Product: ko	nga				
Affected Vers	sion(s): 0.14.9				
N/A	01-May-2023	6.5	An issue discovered in Konga 0.14.9 allows remote attackers to manipulate user accounts regardless of privilege via crafted POST request.	N/A	A-KON-KONG- 170523/586
			CVE ID : CVE-2023- 26987		
Vendor: lazy	y_social_comme	nts_proje	ect		
Product: laz	y_social_comme	ents			
Affected Vers	sion(s): * Up to (i	ncluding)	2.0.4		-
Improper Neutralizat ion of Input During Web Page Generation	09-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Joel James Lazy Social Comments plugin <= 2.0.4 versions.	N/A	A-LAZ-LAZY- 170523/587
('Cross-site Scripting')			CVE ID : CVE-2023- 23733		
Vendor: Lib	ming				
Product: lib	ming				
Affected Vers	sion(s): 0.4.8				
Buffer Copy without Checking Size of Input	09-May-2023	5.5	Buffer Overflow vulnerability found in Libming swftophp v.0.4.8 allows a local attacker to cause a denial of service via	N/A	A-LIB-LIBM- 170523/588
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4 4-5 5-6	6-7 7-8	<u> </u>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer			the newVar_N in util/decompile.c.		
Overflow')			CVE ID : CVE-2023- 30083		
Out-of- bounds Read	09-May-2023	5.5	An issue found in libming swftophp v.0.4.8 allows a local attacker to cause a denial of service via the stackVal function in util/decompile.c.	N/A	A-LIB-LIBM- 170523/589
			CVE ID : CVE-2023- 30084		
Buffer Copy without Checking Size of Input ('Classic Buffer	09-May-2023	5.5	Buffer Overflow vulnerability found in Libming swftophp v.0.4.8 allows a local attacker to cause a denial of service via the cws2fws function in util/decompile.c.	N/A	A-LIB-LIBM- 170523/590
Overflow')			CVE ID : CVE-2023- 30085		
Vendor: ligh	ntspeedhq				
Product: ec	wid_ecommerce	_shoppin	g_cart		
Affected Vers	sion(s): * Up to (e	excluding)	6.11.5		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Ecwid Ecommerce Ecwid Ecommerce Shopping Cart plugin <= 6.11.4 versions. <b>CVE ID : CVE-2023-</b>	N/A	A-LIG-ECWI- 170523/591
Scripting')			24408		
	it_login_attemp		t		
	nit_login_attemp		1.5.0		
Affected Vers	sion(s): * Up to (i	ncluding)	1.7.2		

0-1

1-2

**2-3** 3-4 4-5 Page **306** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	5.4	The Limit Login Attempts WordPress plugin through 1.7.2 does not sanitize and escape usernames when outputting them back in the logs dashboard, which could allow any authenticated users, such as subscriber to perform Stored Cross-Site Scripting attacks <b>CVE ID : CVE-2023-</b> <b>1861</b>	N/A	A-LIM-LIMI- 170523/592
Vendor: Lin	uxfoundation				
Product: flu	id				
Affected Vers	sion(s): From (in	cluding) 0	.7.0 Up to (excluding) 0	.8.6	
Incorrect Authorizati on	08-May-2023	7.8	Fluid is an open source Kubernetes- native distributed dataset orchestrator and accelerator for data-intensive applications. Starting in version 0.7.0 and prior to version 0.8.6, if a malicious user gains control of a Kubernetes node running fluid csi pod (controlled by the `csi-nodeplugin- fluid` node- daemonset), they can leverage the fluid-csi service account to modify specs of all the nodes in the cluster. However, since this service	https://githu b.com/fluid- cloudnative/ fluid/commi t/91c05c32d b131997b5c a065e869c9 918a125c14 9, https://githu b.com/fluid- cloudnative/ fluid/commi t/77c8110a3 d1ec077ae2 bce6bd88d2 96505db155 0	A-LIN-FLUI- 170523/593

0-1

1-2

**2-3** 3-4 4-5 Page **307** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account lacks `list node` permissions, the attacker may need to use other techniques to identify vulnerable nodes.		
			Once the attacker identifies and modifies the node specs, they can manipulate system- level-privileged components to access all secrets in the cluster or execute pods on other nodes. This allows them to elevate privileges beyond the compromised node and potentially gain full privileged access to the whole cluster.		
			To exploit this vulnerability, the attacker can make all other nodes unschedulable (for example, patch node with taints) and wait for system-critical components with high privilege to appear on the compromised node. However, this attack requires two prerequisites: a compromised node		

0-1

1-2

**2-3** 3-4 4-5 Page **308** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and identifying all vulnerable nodes through other means.		
			Version 0.8.6 contains a patch for this issue. As a workaround, delete the `csi-nodeplugin- fluid` daemonset in `fluid-system` namespace and avoid using CSI mode to mount FUSE file systems. Alternatively, using sidecar mode to mount FUSE file systems is recommended.		
			CVE ID : CVE-2023- 30840		
Product: re	kor				
Affected Ver	sion(s): * Up to (e	excluding)	1.1.1	1	
Allocation of Resources Without Limits or Throttling	08-May-2023	7.5	Rekor is an open source software supply chain transparency log. Rekor prior to version 1.1.1 may crash due to out of memory (OOM) conditions caused by reading archive metadata files into memory without checking their sizes first. Verification of a JAR file submitted to Rekor can cause an out of memory crash	https://githu b.com/sigsto re/rekor/co mmit/cf42ac e82667025f e128f7a50cf 6b4cdff51cc 48, https://githu b.com/sigsto re/rekor/sec urity/adviso ries/GHSA- 2h5h-59f5- c5x9	A-LIN-REKO- 170523/594

0-1

1-2

**2-3** 3-4 4-5 Page **309** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			if files within the META-INF directory of the JAR are sufficiently large. Parsing of an APK file submitted to Rekor can cause an out of memory crash if the .SIGN or .PKGINFO files within the APK are sufficiently large. The OOM crash has been patched in Rekor version 1.1.1. There are no known workarounds.		
			CVE ID : CVE-2023- 30551		
Vendor: Llv	m				
Product: llv	m				
Affected Ver	sion(s): 2022-11	-01			
Improper Restriction of Operations within the Bounds of a Memory	05-May-2023	5.5	llvm-project commit fdbc55a5 was discovered to contain a segmentation fault via the component mlir::IROperand <mli r::OpOperand.</mli 	https://githu b.com/llvm/ llvm- project/issu es/58745	A-LLV-LLVM- 170523/595
Buffer			CVE ID : CVE-2023- 29932		
Affected Ver	sion(s): 2022-11	-22			
Out-of- bounds Read	05-May-2023	5.5	llvm-project commit 6c01b5c was discovered to contain a segmentation fault via the component mlir::Type::getDialec t().	https://githu b.com/llvm/ llvm- project/issu es/59136	A-LLV-LLVM- 170523/596

0-1

1-2

2-33-44-5Page 310 of 1106

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29934		
Affected Ver	sion(s): 2022-11	-23			
Reachable Assertion	05-May-2023	5.5	llvm-project commit a0138390 was discovered to contain an assertion failure at !replacements.count( op) && "operation was already replaced.	https://githu b.com/llvm/ llvm- project/issu es/59182	A-LLV-LLVM- 170523/597
			CVE ID : CVE-2023- 29935		
Affected Ver	sion(s): 2022-12	-11			
Out-of- bounds Read	05-May-2023	5.5	llvm-project commit bd456297 was discovered to contain a segmentation fault via the component mlir::Block::getArgu ment. <b>CVE ID : CVE-2023-</b> <b>29933</b>	https://githu b.com/llvm/ llvm- project/issu es/59442	A-LLV-LLVM- 170523/598
Affected Ver	sion(s): 2023-01	-12	29933		
Out-of- bounds Read	05-May-2023	5.5	llvm-project commit a0138390 was discovered to contain a segmentation fault via the component mlir::spirv::TargetEn v::TargetEnv(mlir::s pirv::TargetEnvAttr). <b>CVE ID : CVE-2023- 29939</b>	https://githu b.com/llvm/ llvm- project/issu es/59983	A-LLV-LLVM- 170523/599
Out-of- bounds Read	05-May-2023	5.5	llvm-project commit a0138390 was discovered to contain a	https://githu b.com/llvm/ llvm-	A-LLV-LLVM- 170523/600
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>

Page **311** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			segmentation fault via the component matchAndRewriteSo rtOp <mlir::sparse_te nsor::SortOp&gt;(mlir::s parse_tensor::SortOp CVE ID : CVE-2023-</mlir::sparse_te 	project/issu es/59988	
Out-of- bounds Read	05-May-2023	5.5	29941 llvm-project commit a0138390 was discovered to contain a segmentation fault via the component mlir::Type::isa <mlir:: LLVM::LLVMVoidTyp e. CVE ID : CVE-2023- 29942</mlir:: 	https://githu b.com/llvm/ llvm- project/issu es/59990	A-LLV-LLVM- 170523/601
Vendor: ma	chothemes				
Product: ne	wsmag				
Affected Ver	sion(s): * Up to (i	ncluding)	2.4.4		
Improper Neutralizat ion of Input During Web Page Generation	08-May-2023	5.4	Auth (subscriber+) Reflected Cross-Site Scripting (XSS) vulnerability in Macho Themes NewsMag theme <= 2.4.4 versions.	N/A	A-MAC-NEWS- 170523/602
('Cross-site Scripting')			CVE ID : CVE-2023- 28493		
Vendor: ma	ilbutler				
Product: shi	imo				
Affected Ver	sion(s): 5.0.4				
Improper Authentica tion	04-May-2023	9.8	An issue in the helper tool of Mailbutler GmbH Shimo VPN Client for macOS v5.0.4 allows	N/A	A-MAI-SHIM- 170523/603
					·
	Scale 0-1	L-2 2-3	3-4 4-5 5-6	6-7 7-8	8 8-9 <b>9-10</b>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			attackers to bypass authentication via PID re-use.					
			CVE ID : CVE-2023- 30328					
Vendor: ma	ttermost							
Product: ma	attermost_deskt	ор						
Affected Ver	sion(s): * Up to (i	ncluding)	5.2.2					
URL Redirectio n to Untrusted Site ('Open Redirect')	02-May-2023	5.4	Mattermost Desktop App fails to validate a mattermost server redirection and navigates to an arbitrary website CVE ID : CVE-2023- 2000	https://matt ermost.com/ security- updates	A-MAT-MATT- 170523/604			
Vendor: metaphorcreations								
Product: dit	tty							
Affected Ver	sion(s): * Up to (e	excluding)	3.0.33					
Improper Neutralizat ion of Input During Web Page Generation	03-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Metaphor Creations Ditty plugin <= 3.0.32 versions.	N/A	A-MET-DITT- 170523/605			
('Cross-site Scripting')			CVE ID : CVE-2023- 23874					
Vendor: me	tersphere							
Product: me	etersphere							
Affected Ver	sion(s): * Up to (e	excluding)	2.9.0					
Authorizati on Bypass Through User- Controlled Key	04-May-2023	4.5	MeterSphere is an open source continuous testing platform, covering functions such as test tracking, interface	N/A	A-MET-METE- 170523/606			

· · · · ·			-							
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
			testing, UI testing, and performance testing. This IDOR vulnerability allows the administrator of a project to modify other projects under the workspace. An attacker can obtain some operating permissions. The issue has been fixed in version 2.9.0.		
			CVE ID : CVE-2023- 30550		
Affected Ver	sion(s): 1.20.20-l	ts-79d354	ła6		
N/A	08-May-2023	9.8	Metersphere v1.20.20-lts- 79d354a6 is vulnerable to Remote Command Execution. The system command reverse-shell can be executed at the custom code snippet function of the metersphere system workbench <b>CVE ID : CVE-2023- 29944</b>	N/A	A-MET-METE- 170523/607
Vendor: mic	crobin				
Product: mi	crobin				
Affected Ver	sion(s): 1.2.0				
Improper Neutralizat ion of Input During Web Page Generation	04-May-2023	5.4	A cross-site scripting vulnerability (XSS) in the component microbin/src/pasta.r s of Microbin v1.2.0 allows attackers to execute arbitrary	https://githu b.com/szabo danika/micr obin/pull/14 3	A-MIC-MICR- 170523/608

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			web scripts or HTML via a crafted payload. CVE ID : CVE-2023- 27075		
Vendor: Mi	crosoft			1	
Product: 36	5_apps				
Affected Ver	sion(s): -				
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	A-MIC-365 170523/609
N/A	09-May-2023	3.3	Microsoft Access Denial of Service Vulnerability CVE ID : CVE-2023- 29333	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29333	A-MIC-365 170523/610
Product: ed	lge_chromium				
Affected Ver	sion(s): * Up to (	excluding	) 113.0.1774.35		
N/A	05-May-2023	7.5	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability CVE ID : CVE-2023- 29350	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29350	A-MIC-EDGE- 170523/611
N/A	05-May-2023	4.7	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29354	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29354	A-MIC-EDGE- 170523/612
Product: of	fice				
Affected Ver	sion(s): 2019				
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability	https://msrc .microsoft.co m/update- guide/vulner	A-MIC-OFFI- 170523/613
			3-4 4-5 5-6		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2023- 29335	ability/CVE- 2023-29335						
N/A	09-May-2023	3.3	Microsoft Access Denial of Service Vulnerability CVE ID : CVE-2023- 29333	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29333	A-MIC-OFFI- 170523/614					
Affected Ver	Affected Version(s): 2021									
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	A-MIC-OFFI- 170523/615					
N/A	09-May-2023	3.3	Microsoft Access Denial of Service Vulnerability CVE ID : CVE-2023- 29333	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29333	A-MIC-OFFI- 170523/616					
Product: re	mote_desktop									
Affected Ver	sion(s): * Up to (e	excluding)	10.2.3006.0							
N/A	09-May-2023	5.3	Microsoft Remote Desktop app for Windows Information Disclosure Vulnerability CVE ID : CVE-2023-	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28290	A-MIC-REMO- 170523/617					
			28290							
Product: sh	arepoint_enterp	orise_serv	rer	I						
Affected Ver	sion(s): 2016									
N/A	09-May-2023	6.5	Microsoft SharePoint Server Spoofing Vulnerability CVE ID : CVE-2023- 24950	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24950	A-MIC-SHAR- 170523/618					

CVSS	Scoring	Scale	
------	---------	-------	--

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
Product: sh	arepoint_server	•		<u></u>						
Affected Ver	sion(s): -									
N/A	09-May-2023	6.5	Microsoft SharePoint Server Spoofing Vulnerability CVE ID : CVE-2023- 24950	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24950	A-MIC-SHAR- 170523/619					
Affected Ver	Affected Version(s): 2019									
N/A	09-May-2023	6.5	Microsoft SharePoint Server Spoofing Vulnerability CVE ID : CVE-2023- 24950	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24950	A-MIC-SHAR- 170523/620					
Product: word										
Affected Ver	sion(s): 2016									
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	A-MIC-WORD- 170523/621					
Affected Ver	sion(s): 2013			·						
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	A-MIC-WORD- 170523/622					
Vendor: mo	nicahq									
Product: mo	onica									
Affected Ver	sion(s): 4.0.0									
N/A	08-May-2023	8.8	MonicaHQ version 4.0.0 allows an authenticated remote attacker to execute malicious code in the	N/A	A-MON-MONI- 170523/623					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	Page <b>317</b> of <b>1106</b>									

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application via CSTI in the `people:id/food` endpoint and food parameter.		
			CVE ID : CVE-2023- 1094		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	MonicaHQ version 4.0.0 allows an authenticated remote attacker to execute malicious code in the application via CSTI in the `people:id/introducti ons` endpoint and first_met_additional_ info parameter. <b>CVE ID : CVE-2023-</b>	https://ww w.monicahq. com/	A-MON-MONI- 170523/624
			30787		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	MonicaHQ version 4.0.0 allows an authenticated remote attacker to execute malicious code in the application via CSTI in the `people/add` endpoint and nickName, description, lastName, middleName and firstName parameter. <b>CVE ID : CVE-2023-</b> <b>30788</b>	https://ww w.monicahq. com/	A-MON-MONI- 170523/625
Improper Neutralizat ion of Input	08-May-2023	5.4	MonicaHQ version 4.0.0 allows an authenticated remote attacker to	https://ww w.monicahq. com/	A-MON-MONI- 170523/626

0-1

1-2

**2-3** 3-4 4-5 Page **318** of **1106**  5-6

6-7

7-8

During Web Page Generation ('Cross-site Scripting')			execute malicious code in the application via CSTI		
			in the `people:id/work` endpoint and job and company parameter.		
			CVE ID : CVE-2023- 30789		
Improper Neutralizat ion of Input During 0 Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	MonicaHQ version 4.0.0 allows an authenticated remote attacker to execute malicious code in the application via CSTI in the `people:id/relationsh ips` endpoint and first_name and last_name parameter. <b>CVE ID : CVE-2023-</b> <b>30790</b>	https://ww w.monicahq. com/	A-MON-MONI- 170523/627
Vendor: Mood	dle				
Product: moo	odle				
Affected Versio	on(s): From (ind	cluding) 3	.11.0 Up to (excluding)	3.11.14	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user- supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands	https://moo dle.org/mod /forum/disc uss.php?d=4 46286, https://bugz illa.redhat.co m/show_bug .cgi?id=2188 606, http://git.m oodle.org/g w?p=moodle .git&a=searc h&h=HEAD&	A-MOO-MOOD- 170523/628
CVSS Scoring Sca	ale 0-1 1	2 2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page **319** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			within the application database. CVE ID : CVE-2023- 30944	st=commit& s=MDL- 77187	
Affected Ver	sion(s): From (in	cluding) 3	.9.0 Up to (excluding) 3	.9.21	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user- supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database. <b>CVE ID : CVE-2023- 30944</b>	https://moo dle.org/mod /forum/disc uss.php?d=4 46286, https://bugz illa.redhat.co m/show_bug .cgi?id=2188 606, http://git.m oodle.org/g w?p=moodle .git&a=searc h&h=HEAD& st=commit& s=MDL- 77187	A-M00-M00D- 170523/629
Affected Ver	sion(s): From (in	cluding) 4	.0.0 Up to (excluding) 4	.0.8	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user- supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database.	https://moo dle.org/mod /forum/disc uss.php?d=4 46286, https://bugz illa.redhat.co m/show_bug .cgi?id=2188 606, http://git.m oodle.org/g w?p=moodle .git&a=searc h&h=HEAD& st=commit&	A-M00-M00D- 170523/630

0-1

1-2

**2-3** 3-4 4-5 Page **320** of **1106**  5-6

6-7

Affected Vers					
Affected Vers			CVE ID : CVE-2023- 30944	s=MDL- 77187	
	ion(s): From (in	cluding) 4	.1.0 Up to (excluding) 4	.1.3	
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user- supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database. <b>CVE ID : CVE-2023- 30944</b>	https://moo dle.org/mod /forum/disc uss.php?d=4 46286, https://bugz illa.redhat.co m/show_bug .cgi?id=2188 606, http://git.m oodle.org/g w?p=moodle .git&a=searc h&h=HEAD& st=commit& s=MDL- 77187	A-MOO-MOOD- 170523/631
Externally Controlled Reference to a Resource in Another Sphere	02-May-2023	5.3	The vulnerability was found Moodle which exists because the application allows a user to control path of the older to create in TinyMCE loaders. A remote user can send a specially crafted HTTP request and create arbitrary folders on the system. <b>CVE ID : CVE-2023-</b> <b>30943</b>	http://git.m oodle.org/g w?p=moodle .git&a=searc h&h=HEAD& st=commit& s=MDL- 77718, https://moo dle.org/mod /forum/disc uss.php?d=4 46285, https://bugz illa.redhat.co m/show_bug .cgi?id=2188 605	A-MOO-MOOD- 170523/632
Vendor: mul	ti_language_ho	tel_mana	gement_software_proj	ect	
Product: mu	lti_language_ho	tel_mana	gement_software		
CVSS Scoring Sc	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				
Affected Version(s): 1.0									
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	07-May-2023	6.1	A vulnerability has been found in SourceCodester Multi Language Hotel Management Software 1.0 and classified as problematic. This vulnerability affects unknown code of the file ajax.php of the component POST Parameter Handler. The manipulation of the argument complaint_type with the input <script>alert(docum ent.cookie)</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- 228172. <b>CVE ID : CVE-2023-</b> <b>2565</b>	N/A	A-MUL-MULT- 170523/633				
Vendor: mu	tagen								
Product: mu									
Affected Version(s): * Up to (excluding) 0.16.6									
Improper Encoding or Escaping of Output	08-May-2023	8.8	Mutagen provides real-time file synchronization and flexible network forwarding for developers. Prior to versions 0.16.6 and	https://githu b.com/muta gen- io/mutagen/ security/adv isories/GHS	A-MUT-MUTA- 170523/634				
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10									

Page 322 of 1106

0-1

1-2

2-33-44-5Page 323 of 1106

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			patched. Versions of Mutagen after v0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk. <b>CVE ID : CVE-2023-</b>					
			30844					
Affected Version(s): 0.17.0								
Improper Encoding or Escaping of Output	08-May-2023	8.8	Mutagen provides real-time file synchronization and flexible network forwarding for developers. Prior to versions 0.16.6 and 0.17.1 in `mutagen` and prior to version 0.17.1 in `mutagen- compose`, Mutagen `list` and `monitor` commands are susceptible to control characters that could be provided by remote endpoints. This could cause terminal corruption, either intentional or unintentional, if these characters were present in error messages or file paths/names. This could be used as an attack vector if	https://githu b.com/muta gen- io/mutagen/ security/adv isories/GHS A-jmp2- wc4p-wfh2	A-MUT-MUTA- 170523/635			

0-1

1-2

**2-3** 3-4 4-5 Page **324** of **1106**  5-6

synchronizing with an untrusted remote endpoint, synchronizing files not under control of the user, or forwarding to/from an untrusted remote endpoint. On very old systems with terminals susceptible to issues such as CVE-2003-0069, the issue could theoretically cause code execution. The problem has been patched in Mutagen v0.16.6 and v0.17.1. Earlier versions of Mutagen arter v0.18.0 will also have the patched. Versions of Mutagen arter v0.18.0 will also have the patched with untrusted files or interaction with untrusted remote endpoints should mitigate any risk. CVE ID : CVE-2023- 30844     Https://githu b.com/muta gen- io/mutagen/ A-MUT-MUTA- 170523/636	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mutagen_compose       04       12       24       34       45       56       67       74       84       242				synchronizing with		
Product: mutger_compose       8.8       Mutagen provides the provides of the				an untrusted remote		
Product       mot under control of the user, or or forwarding to/from an untrusted remote endpoint. On very old systems with terminals susceptible to issues such as CVE-2003-0069, the issue could theoretically cause code execution. The problem has been patched in Mutagen v0.16.6 and v0.17.1. Earlier versions of Mutagen are no longer supported and will not be patched. Versions of Mutagen after v0.18.0 will also have the patch endge As a workaround, avoiding synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk. CVE ID : CVE-2023-30844         Product:       mutagen_compose         Affected Versions (s): * Up to (excluding) 0.17.1         Improper Encoding or 08-May-2023       8.8         Matagen provides synchronization and flexible network       https://githu bicom/mutagen/io/mut				endpoint,		
Product: mutagen_compose       8.8       Mutagen provides space moves in figure of the figure				synchronizing files		
Product: mutagen_compose       Ba       Mutagen provides read-time file good       https://gith b.com/mutagen       A-MUT-MUTA-170523/636         Mutagen are no longer supported and will not be patched. Versions of Mutagen are no longer supported and will not be patched. Versions of Mutagen are no longer supported and will not be patched. Versions of Mutagen after v0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted remote endpoints should mitigate any risk.       CVE-2023-30644       A       A       A       A       A/UT-MUTA-170523/636       A       A       A       A       A/UT-MUTA-170523/636       A       A       4       5       6       7       7.8       8.9       940				not under control of		
an untrusted remote endpoint. On very old systems with terminals susceptible to issues such as CVE-2003-0069, the issue could theoretically cause code execution. The problem has been patched in Mutagen v0.16.6 and v0.17.1. Earlier versions of Mutagen are no longer supported and will not be patched. Versions of Mutagen after v0.18.0 will also have the patched. Versions of Mutagen after v0.18.0 will also have the patched wersion of untrusted files or interaction with untrusted remote endpoints should mitigate any risk. CVE ID: CVE-2023- 30844       Image: Compose of the support of ad workaround, avoiding synchronization of untrusted remote endpoints should mitigate any risk.       Image: Compose of the support of ad workaround, avoiding synchronization and fexible network       Image: Compose https://githu b.com/mutagen.       A-MUT-MUTA- 170523/636				the user, or		
Product: mutagen_compose       endpoint. On very old systems with terminals susceptible to issues such as CVE-2003-0069, the issue could theoretically cause code execution. The problem has been patched in Mutagen v0.16.6 and v0.17.1.       Image: Compose of the terminal code execution. The problem has been patched. In Mutagen v0.16.6 and v0.17.1.         Earlier versions of Mutagen are no longer supported and will not be patched. Versions of Mutagen after v0.18.0 will also have the patched. Version after the patched. Version after the patched. Version after the patched. Version after the patched. Ver				forwarding to/from		
old systems with terminals susceptible to issues such as CVE-2003-0069, the issue could theoretically cause code execution. The problem has been patched in Mutagen v0.16.6 and v0.17.1. Earlier versions of Mutagen are no longer supported and will not be patched. Versions of Mutagen after v0.18.0 will also have the patch Murgen after v0.18.0 will also have the patched. Versions of Mutagen after v0.18.0 will also have the patched. Versions of Mutagen after v0.18.0 will also have the patched with untrusted and will not be patched. Versions of Mutagen after v0.18.0 will also have the patch Murgen after v0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted fles or interaction with untrusted fremote endpoints should mitigate any risk. CVE ID : CVE-2023- 30844       Versions Versions A Mutagen provides real-time file synchronization and flexible network       https://githu b.com/muta gen- io/mutagen/       A-MUT-MUTA- 170523/636				an untrusted remote		
Product: mutagen_compose       08-May-2023       8.8       8.8       Value of the full source of t				endpoint. On very		
to issues such as CVE-2003-0069, the issue could theoretically cause code execution. The problem has been patched in Mutagen patched in Mut				old systems with		
CVE-2003-0069, the       issue could       theoretically cause       code execution. The         problem has been       patched in Mutagen       v0.16.6 and v0.17.1.       Earlier versions of         Mutagen are no       longer supported       and will not be       patched. Versions of         Mutagen are no       longer supported       and will not be       patched. Versions of         Mutagen after       v0.18.0 will also have       the patchen erged. As       a workaround,         avoiding       synchronization of       untrusted files or       interaction with         untrusted remote       endpoints should       mitigate any risk.       CVE ID : CVE-2023-         CVEE DI : CVE-2023-       30844       somy       A-MUT-MUTA-         Improper       08-May-2023       8.8       Mutagen provides real-time file synchronization and flexible network       https://githu b.com/muta gen-         cvss Scoring Scale       04       12       24       34       4-5       5-6       6-7       7.8       8-9       940				terminals susceptible		
read       issue could       issue could       issue could       issue could       iteoretically cause       code execution. The problem has been patched in Mutagen avoide and wull act be       issue could       isu				to issues such as		
Product: mutagen_compose       08-May-2023       8.8       Mutagen provides real-time file synchronization and results       https://githu b.com/mutagen/io//mutagen/io/mutagen				CVE-2003-0069, the		
code execution. The problem has been patched in Mutagen v0.16.6 and v0.17.1. Earlier versions of Mutagen are no longer supported and will not be patched. Versions of Mutagen after v0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted files or interaction with untrusted files or interaction with untrusted remote endpoints should mitigate any risk.elaaaProduct: mutagen_compose suported and will and will not be patched. Versions of Mutagen after v0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk. CVE ID : CVE-2023- 30844				issue could		
Product: mutagen_compose       08-May-2023       8.8       Mutagen provides real-time file synchronization and gen-io/mutagen       https://githu b.com/muta gen-io/mutagen         CVSS Scoring Scale       04       12       23       34       4-5       5-6       6-7       7-8       8-9       9.00				=		
Patched in Mutagen       v0.16.6 and v0.17.1.         Earlier versions of       Mutagen are no         longer supported       and will not be         patched. Versions of       Mutagen after         v0.18.0 will also have       the patch merged. As         a workaround,       avoiding         synchronization of       untrusted files or         interaction with       untrusted files or         interaction with       untrusted files or         interaction with       untrusted remote         endpoints should       mitigate any risk.         CVE ID : CVE-2023-       30844         Product: mutagen_compose       Mutagen provides         Affected Version(s): * Up to (excluding) 0.17.1       Mutagen provides         Improper       08-May-2023       8.8         Base       Mutagen provides         real-time file       synchronization and         gen-       io/mutagen/         io/mutagen/       170523/636						
v0.16.6 and v0.17.1.         Earlier versions of         Mutagen are no         longer supported         and will not be         patched. Versions of         Mutagen after         v0.18.0 will also have         the patch merged. As         a workaround,         avoiding         synchronization of         untrusted files or         interaction with         untrusted remote         endpoints should         mitigate any risk.         CVE ID : CVE-2023-         30844    Product: mutagen_compose Affected Version(s): * Up to (excluding) 0.17.1          Improper         Encoding         or         08-May-2023         8.8         Mutagen provides         real-time file         synchronization and         fexible network         io/mutagen/				1		
Earlier versions of Mutagen are no longer supported and will not be patched. Versions of Mutagen after v0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk.Image: Compose mutagen are no longer supported and will not be patched. Versions of Mutagen after w0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk.Image: Compose mutagenProduct: mutagen_composeMutagen provides real-time file synchronization and flexible networkhttps://githu b.com/muta gen- io/mutagen/A-MUT-MUTA- 170523/636						
Product: mutagen_compose       Mutagen are no       by patched. Versions of       Mutagen after       v0.18.0 will also have       by patched. Versions of       Mutagen after       v0.18.0 will also have       by patched. Versions of       Mutagen after       v0.18.0 will also have       by patched. Versions of       Mutagen after       v0.18.0 will also have       by patched. Versions of       Mutagen after       v0.18.0 will also have       by patched. Versions of       Mutagen after       v0.18.0 will also have       by patched. Versions of       Mutagen after       v0.18.0 will also have       by patched. Versions of       Mutagen after       v0.18.0 will also have       by patched. Versions of       Mutagen are no       by patched. Versions of       by patched. Versions of       by patched. Versions of       Mutagen are no       by patched. Versions of       by patched.						
Product: mutagen_composeMutagen provides a workaround, avoiding synchronization of untrusted files or interaction with untrusted files or interaction with untrusted remote endpoints should mitigate any risk.https://githu gen- io/mutagen/A-MUT-MUTA- 170523/636Product: mutagen_composeMutagen provides real-time file synchronization and flexible networkhttps://githu gen- io/mutagen/A-MUT-MUTA- 170523/636				Earlier versions of		
Product: mutagen_composeAffected Version(s): * Up to (excluding) 0r08-May-2023 or08-May-2023 or0411224344556677889910				-		
patched. Versions of Mutagen after v0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted files or interaction with untrusted files or interaction with untrusted remote endpoints should mitigate any risk.Image: Compose of the patch merged of the pa						
Mutagen after v0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk. CVE ID : CVE-2023- 30844Image: CVE ID image: CVE						
v0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk.Image in the synchronization of untrusted remote endpoints should mitigate any risk.Product: mutagen_composeVO.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk.Image in the synchronization of untrusted remote endpoints should mitigate any risk.Mutagen provides synchronization and gen- io/mutagen/A-MUT-MUTA- 170523/636UVSS Scoring Scale011-22-33-44-55-66-77-88-99-10				-		
Product: mutzgen_compose Encoding or08-May-20238.8BasMutagen provides real-time file synchronization and flexible networkhttps://githu b.com/muta gen- io/mutagen/A-MUT-MUTA- 170523/636CVSS Scoring Scale011-22.33.44-55-66-77-88-99.10				_		
a workaround, avoiding synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk.       Image: State St						
A-MUT-MUTA-   Improper   Encoding   08-May-2023   8.8   Mutagen provides   https://githu   b.com/muta   gen-   io/mutagen/     A-MUT-MUTA-   170523/636						
with a synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk.       with a synchronization of untrusted remote endpoints should mitigate any risk.         CVE ID : CVE-2023-30844       CVE ID : CVE-2023-30844         Product: mutagen_compose       0.17.1         Improper Encoding or       08-May-2023       8.8       Mutagen provides real-time file synchronization and flexible network       https://githu b.com/muta gen-io/mutagen/io						
VersionNumberNumberNumberNumberImproper Encoding or08-May-20238.8Mutagen provides synchronization and flexible networkhttps://githu b.com/muta gen- io/mutagen/A-MUT-MUTA- 170523/636CVSS Scoring Scale0-11-22-33-44-55-66-77-88-99-10				U		
Improper Encoding or08-May-20238.8Mutagen provides synchronization and flexible networkhttps://githu b.com/muta gen- io/mutagen/A-MUT-MUTA- 170523/636CVSS Scoring Scale0-11-22-33-44-55-66-77-88-99-10				-		
Improper Encoding or08-May-20238.8Mutagen provides real-time file synchronization and flexible networkhttps://githu b.com/muta gen- io/mutagen/A-MUT-MUTA- 170523/636CVSS Scoring Scale0-11-22-33-44-55-66-77-88-99-10						
endpoints should mitigate any risk.endpoints shou						
mitigate any risk. CVE ID : CVE-2023- 30844mitigate any risk. CVE ID : CVE-2023- 30844Product: mutagen_composeVerture sourceMutagen provides real-time file synchronization and flexible networkhttps://githu b.com/muta gen- io/mutagen/A-MUT-MUTA- 170523/636Mutagen providesNutagen provides real-time file synchronization and flexible networkhttps://githu b.com/muta gen- io/mutagen/A-MUT-MUTA- 170523/636						
CVE ID : CVE-2023- 30844       CVE ID : CVE-2023- 30844         Product: mutagen_compose         Affected Version(s): * Up to (excluding) 0.17.1         Improper Encoding or       08-May-2023       8.8       Mutagen provides real-time file synchronization and flexible network       https://githu b.com/muta gen- io/mutagen/       A-MUT-MUTA- 170523/636				_		
Improper Encoding or $08$ -May-2023 $8.8$ Mutagen provides real-time file synchronization and flexible networkhttps://githu b.com/muta gen- io/mutagen/ $A$ -MUT-MUTA- 170523/636CVSS Scoring Scale0-11-22-33-44-55-66-77-88-99-10				с .		
Product: mutagen_compose       Affected Version(s): * Up to (excluding) 0.17.1         Improper Encoding or       08-May-2023       8.8       Mutagen provides real-time file synchronization and flexible network       https://githu b.com/muta gen- io/mutagen/       A-MUT-MUTA- 170523/636         CVSS Scoring Scale       0-1       1-2       2-3       3-4       4-5       5-6       6-7       7-8       8-9       9-10						
Affected Version(s): * Up to (excluding) 0.17.1         Improper Encoding or       08-May-2023       8.8       Mutagen provides real-time file synchronization and flexible network       https://githu b.com/muta gen-io/mutagen/				30844		
Improper Encoding or       08-May-2023       8.8       Mutagen provides real-time file synchronization and flexible network       https://githu b.com/muta gen- io/mutagen/       A-MUT-MUTA- 170523/636         CVSS Scoring Scale       0-1       1-2       2-3       3-4       4-5       5-6       6-7       7-8       8-9       9-10						
Improper Encoding or       08-May-2023       8.8       real-time file synchronization and flexible network       b.com/muta gen- io/mutagen/       A-MUT-MUTA- 170523/636         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 (	excluding)	0.17.1		
Encoding or       08-May-2023       8.8       real-time file synchronization and flexible network       b.com/muta gen-io/mutagen/       A-MOT-MOTA         CVSS Scoring Scale       0-1       1-2       2-3       3-4       4-5       5-6       6-7       7-8       8-9       9-10	Improper					
Inteoding orysynchronization and flexible networkgen- io/mutagen/170523/636CVSS Scoring Scale0-11-22-33-44-55-66-77-88-99-10		08-Mav-2023	8.8		b.com/muta	
Image: State       Image: State <th< td=""><td>0</td><td></td><td></td><td>-</td><td>gen-</td><td>170523/636</td></th<>	0			-	gen-	170523/636
	51			flexible network	io/mutagen/	
	CVSS Scoring S	scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>325</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Escaping of			forwarding for	security/adv	
Output			developers. Prior to	isories/GHS	
			versions 0.16.6 and	A-jmp2-	
			0.17.1 in `mutagen`	wc4p-wfh2	
			and prior to version		
			0.17.1 in `mutagen-		
			compose`, Mutagen		
			`list` and `monitor`		
			commands are		
			susceptible to		
			control characters		
			that could be		
			provided by remote		
			endpoints. This		
			could cause terminal		
			corruption, either		
			intentional or		
			unintentional, if		
			these characters		
			were present in		
			error messages or		
			file paths/names.		
			This could be used as		
			an attack vector if		
			synchronizing with		
			an untrusted remote		
			endpoint,		
			synchronizing files		
			not under control of		
			the user, or		
			forwarding to/from		
			an untrusted remote		
			endpoint. On very		
			old systems with		
			terminals susceptible to issues such as		
			CVE-2003-0069, the issue could		
			theoretically cause		
			code execution. The		
			problem has been		
			patched in Mutagen		
			v0.16.6 and v0.17.1.		
			Earlier versions of		

0-1

1-2

**2-3** 3-4 4-5 Page **326** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mutagen are no longer supported and will not be patched. Versions of Mutagen after v0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk. <b>CVE ID : CVE-2023-</b>		
			30844		
Vendor: net					
-	plication_securi	ty_gatewa	ay		
Affected Ver			NS-ASG v6.3 was		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	05-May-2023	9.8	NS-ASG V6.3 Was discovered to contain a SQL injection vulnerability via the component /admin/add_ikev2.p hp. CVE ID : CVE-2023- 30242	N/A	A-NET-APPL- 170523/637
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	05-May-2023	7.5	Beijing Netcon NS- ASG Application Security Gateway v6.3 is vulnerable to SQL Injection via TunnelId that allows access to sensitive information. <b>CVE ID : CVE-2023-</b> <b>30243</b>	N/A	A-NET-APPL- 170523/638
	wbee-mall_proje	ect			
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5-6	6-7 7-8	8 8-9 <mark>9-10</mark>

Page 327 of 1106

Weakness	Publish Date	CVSSv3	Descripti	on & CVE	ID	Patch		NCIIP	C ID
Product: ne	wbee-mall								
Affected Ver	sion(s): * Up to (e	excluding)	2022-10-2	27					
Authorizati on Bypass Through User- Controlled Key	04-May-2023	5.4	Insecure j in the updateUs function of mall befor 1f2c2dfy attackers user acco informati <b>CVE ID : 0</b> <b>30216</b>	erInfo of newbe re comm allows to obtai unt on.	ee- nit n	N/A		A-NEW-N 170523/	
Vendor: nev	wbinggogo_proj	ect							
Product: ne									
	sion(s): * Up to (i	ncluding)	2023.5.5.2						
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	6.1	A vulnera found in j NewBing 2023.5.5. been rate problema issue affe unknown The mani leads to c scripting. may be in remotely. has been the public be used. T associated of this vul is VDB-22 <b>CVE ID : C</b> 2560	ja8 GoGo up 2. It has d as tic. This cts some process pulation ross site The atta itiated The exp disclose and ma he d identif nerabili 28167.	to e sing. ack bloit d to y ïer ty	N/A		A-NEW-N 170523/	
Vendor: obs	Vendor: obsidian								
Product: ob	Product: obsidian								
Affected Ver	Affected Version(s): 1.1.9								
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

variable preview function/2023/sa20 23-07/1/0523/642Affected Version(s): From (including) 2022.4.0 Up to (excluding) 2022.4.8319In affected versions of Octopus Deploy it is possible to unmask variablehttps://advi sories.octopA-OCT-OCTO-	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Product: octopus_deployAffected Version(s): From (i=104 ding) 2018.3.0 Up to (excluding) 2022.3.10929N/A02-May-2023In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview 2023/sa20 23-07/https://advi sories.octop us.com/post /2023/sa20 23-07/A-OCT-OCTO- 170523/642Affected Version(s): From (i=104 ding)CVE ID : CVE-2023- 22472022.4.8319A-OCT-OCTO- 170523/642Affected Version(s): From (i=104 ding)In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview variable preview variable preview (2023/sa20) 23-07/A-OCT-OCTO- 170523/642N/A02-May-20235.3In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview variable preview variable preview (2023/sa20) 23-07/A-OCT-OCTO- 170523/643N/A02-May-20235.3In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview (2023/sa20) 23-07/A-OCT-OCTO- 170523/643N/A02-May-20235.3In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview (2023/sa20) 23-07/A-OCT-OCTO- 170523/643N/A02-May-20235.3In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview 2023/sa20 23-07/A-OCT-OCTO- 170523/643N/A02-May-20235.3Im affected versions of Octop	Default Permission	01-May-2023	7.5	in Obsidian Canvas 1.1.9 allows remote attackers to send desktop notifications, record user audio and other unspecified impacts via embedded website on the canvas page. <b>CVE ID : CVE-2023-</b>	N/A		
Affected Version(s): From (including) 2018.3.0 Up to (excluding) 2022.3.10929N/A02-May-20235.3In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview function CVE ID : CVE-2023- 2247https://advi scom/post /2023/sa20 23-07/A-OCT-OCTO- 170523/642Affected Version(s): From (including) 2022.4.0 Up to (excluding) 2022.4.8319CVE ID : CVE-2023- 2247S.3In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview functionN/AO2-May-2023S.3In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview functionN/AA-OCT-OCTO- 170523/642N/A02-May-20235.3In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview function CVE ID : CVE-2023- 	Vendor: oct	opus			1		
N/A02-May-20235.3In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview functionhttps://advi sories.octop us.com/post /2023/sa20 23-07/A-OCT-OCTO- 170523/642Affected Version(s): From (including)2V22.4.0 Up to (excluding)2022.4.8319M/A02-May-20235.3In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview functionIn affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview functionA-OCT-OCTO- 170523/642N/A02-May-20235.3In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview functionhttps://advi sories.octop us.com/post /2023/sa20 23-07/A-OCT-OCTO- 170523/643N/A02-May-20235.3In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview functionhttps://advi sories.octop us.com/post /2023/sa20 23-07/A-OCT-OCTO- 170523/643Vendor: olevmedia_shortcodesVertureVertureVertureVertureVerdor: olevmedia_shortcodes	Product: oc	topus_deploy					
N/A02-May-20235.3of Octopus Deploy it is possible to unmask variable secrets using the variable preview functionhttps://advi sories.octop us.com/post /2023/sa20 23-07/A-OCT-OCTO- 170523/642Affected Versions N/A02-May-2023Imaffected Versions of Octopus Deploy it is possible to unmask variable sories.octop of Octopus Deploy it is possible to unmask variable secrets using the variable preview of Octopus Deploy it is possible to unmask variable secrets using the variable preview functionhttps://advi sories.octop us.com/post /2023/sa20 23-07/N/A02-May-20235.3Imaffected Versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview functionhttps://advi sories.octop us.com/post /2023/sa20 23-07/A-OCT-OCTO- 170523/642N/A02-May-20235.3Imaffected Versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview functionhttps://advi sories.octop us.com/post /2023/sa20 23-07/Vendor: oterwediaUUUUVerdor: oterwedia-secretsus	Affected Ver	sion(s): From (in	cluding) 2	018.3.0 Up to (excludin	g) 2022.3.1092	9	
N/A02-May-20235.3In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview functionhttps://advi sories.octop us.com/post /2023/sa20 23-07/A-OCT-OCTO- 170523/643Vendor: olevmediaVendor: olevmedia_shortcodesIn affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview functionhttps://advi sories.octop us.com/post /2023/sa20 23-07/A-OCT-OCTO- 170523/643Vendor: olevmediaProduct: olevmedia_shortcodesIn affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview functionhttps://advi sories.octop us.com/post /2023/sa20 23-07/A-OCT-OCTO- 170523/643	N/A	02-May-2023	5.3	of Octopus Deploy it is possible to unmask variable secrets using the variable preview function <b>CVE ID : CVE-2023-</b>	sories.octop us.com/post /2023/sa20		
N/A02-May-20235.3of Octopus Deploy it is possible to unmask variable secrets using the variable preview functionhttps://advi sories.octop us.com/post /2023/sa20 23-07/A-OCT-OCTO- 170523/643Vendor: olewedia_shortcodes	Affected Ver	sion(s): From (in	cluding) 2	022.4.0 Up to (excludin	g) 2022.4.8319		
Product: olevmedia_shortcodes	N/A	02-May-2023	5.3	of Octopus Deploy it is possible to unmask variable secrets using the variable preview function <b>CVE ID : CVE-2023-</b>	sories.octop us.com/post /2023/sa20		
	Vendor: olevmedia						
Affected Version(s): * Up to (including) 1.1.9	Product: ole	Product: olevmedia_shortcodes					
	Affected Ver	sion(s): * Up to (i	ncluding)	1.1.9			

0-1

1-2

**2-3** 3-4 4-5 Page **329** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Olevmedia Olevmedia Shortcodes plugin <= 1.1.9 versions. <b>CVE ID : CVE-2023-</b>	N/A	A-OLE-OLEV- 170523/644
Vendor: on	line_dj_manager	nont syst	25798		
	line_dj_manage				
Affected Ver	- /- 0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	01-May-2023	9.8	A vulnerability was found in SourceCodester Online DJ Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/bookings/vi ew_details.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB- 227795. <b>CVE ID : CVE-2023-</b> 2451	N/A	A-ONL-ONLI- 170523/645

0-1

1-2

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: onl	ine_food_order	ng_syster	m_project	I	
Product: on	line_food_order	ing_syste	m		
Affected Ver	sion(s): 2.0				
Unrestricte d Upload of File with Dangerous Type	05-May-2023	9.8	An arbitrary file upload vulnerability in the component /admin/ajax.php?act ion=save_menu of Online Food Ordering System v2.0 allows attackers to execute arbitrary code via uploading a crafted PHP file. <b>CVE ID : CVE-2023-</b> <b>30122</b>	N/A	A-ONL-ONLI- 170523/646
Vendor: onl	ine_pizza_order	ing_syste	em_project		
	line_pizza_orde				
Affected Ver		89	-		
Improper					
Neutralizat ion of Special Elements used in an SQL Command	08-May-2023	9.8	SourceCodester Online Pizza Ordering System v1.0 is vulnerable to SQL Injection via the QTY parameter. <b>CVE ID : CVE-2023-</b>	N/A	A-ONL-ONLI- 170523/647
('SQL			30092		
Injection')	ine_reviewer_sy	istem nr	niect		
	line_reviewer_sy				
Affected Ver		Jucin			
Improper			A vulnerability was		
Neutralizat ion of Special	09-May-2023	9.8	found in SourceCodester Online Reviewer	N/A	A-ONL-ONLI-
Elements used in an SQL Command			System 1.0 and classified as critical. Affected by this issue is some unknown		170523/648
communu					
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')			functionality of the file /reviewer/system/s ystem/admins/mana ge/users/user- update.php of the component GET Parameter Handler. The manipulation of the argument user_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-228398 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023- 2596</b>		
Vendor: onl	ine_tours_\&_tr	avels_ma	nagement_system_pro	oject	
			anagement_system		
Affected Ver	sion(s): 1.0				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	10-May-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Online Tours & Travels Management System 1.0. This affects the function exec of the file disapprove_delete.ph p. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to	N/A	A-ONL-ONLI- 170523/649

0-1

1-2

2-33-44-5Page 332 of 1106

5-6

6-7

7-8 8-9

Improper Neutralizat ion of Input		the public and may be used. The identifier VDB- 228549 was assigned to this vulnerability. <b>CVE ID : CVE-2023-</b> <b>2619</b> <b>1.9.0 Up to (including) 2.</b> A cross-site scripting	7.0	
Product: onosAffected Version(s)Improper Neutralizat ion of Input During04-Ma 04-Ma 04-Ma 04-Ma		2619 1.9.0 Up to (including) 2.	7.0	
Product: onosAffected Version(s)Improper Neutralizat ion of Input During04-Ma 04-Ma 04-Ma			7.0	
Affected Version(s) Improper Neutralizat ion of Input During Web Page Generation	: From (including)		7.0	
Improper Neutralizat ion of Input During Web Page Generation	: From (including)		7.0	
Neutralizat ion of Input During 04-Ma Web Page Generation		A cross-site scripting	7.0	
Scripting')	ay-2023 6.1	<ul> <li>(XSS) vulnerability in</li> <li>Open Networking</li> <li>Foundation ONOS</li> <li>from version v1.9.0</li> <li>to v2.7.0 allows</li> <li>attackers to execute</li> <li>arbitrary web scripts</li> <li>or HTML via a</li> <li>crafted payload</li> <li>injected into the url</li> <li>parameter of the API</li> <li>documentation</li> <li>dashboard.</li> </ul>	N/A	A-ONO-ONOS- 170523/650
		30093		
Vendor: Open-emi				
Product: openemr				
Affected Version(s)	: • Up to (excludin	gj /.U.1	1	
Improper Neutralizat ion of Input During 08-Ma Web Page Generation ('Cross-site Scripting')	ay-2023 4.8	Cross-site Scripting (XSS) - Stored in GitHub repository openemr/openemr prior to 7.0.1. CVE ID : CVE-2023- 2566	https://githu b.com/opene mr/openemr /commit/a2 adac7320dfc 631b1da688 c3b04f54b8 240fc7b, https://hunt r.dev/bounti es/47d6fc2a	A-OPE-OPEN- 170523/651
CVSS Scoring Scale	0-1 1-2 2	2-3 3-4 4-5 5-6	6-7 7-8	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-989a-44eb- 9cb7- ab4f8bd444 96	
Vendor: op	enproject				
Product: op	enproject				
Affected Ver	sion(s): From (in	cluding) 7	4.0 Up to (excluding) 1	2.5.4	
Insufficient Session Expiration	08-May-2023	6.5	OpenProject is open source project management software. Starting with version 7.4.0 and prior to version 12.5.4, when a user registers and confirms their first two-factor authentication (2FA) device for an account, existing logged in sessions for that user account are not terminated. Likewise, if an administrators creates a mobile phone 2FA device on behalf of a user, their existing sessions are not terminated. The issue has been resolved in OpenProject version 12.5.4 by actively terminating sessions of user accounts having registered and confirmed a 2FA device. As a workaround, users who register the first 2FA device on their account can	https://githu b.com/opf/o penproject/s ecurity/advi sories/GHSA -xfp9-qqfj- x28q, https://githu b.com/opf/o penproject/ pull/12508	A-OPE-OPEN- 170523/652

0-1

1-2

**2-3** 3-4 4-5 Page **334** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manually log out to terminate all other active sessions. This is the default behavior of OpenProject but might be disabled through a configuration option. Double check that this option is not overridden if one plans to employ the workaround. <b>CVE ID : CVE-2023-</b>		
Vendor: ope	antsdh		31140		
Product: op					
-		cluding) 1	.0.0 Up to (including) 2	.4.1	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	03-May-2023	9.8	Due to insufficient validation of parameters passed to the legacy HTTP query API, it is possible to inject crafted OS commands into multiple parameters and execute malicious code on the OpenTSDB host system. This exploit exists due to an incomplete fix that was made when this vulnerability was previously disclosed as CVE-2020-35476. Regex validation that was implemented to restrict allowed	https://githu b.com/Open TSDB/opent sdb/pull/22 75	A-OPE-OPEN- 170523/653

0-1

1-2

2-33-44-5Page 335 of 1106

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input to the query API does not work as intended, allowing crafted commands to bypass validation.		
			CVE ID : CVE-2023- 25826		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Due to insufficient validation of parameters reflected in error messages by the legacy HTTP query API and the logging endpoint, it is possible to inject and execute malicious JavaScript within the browser of a targeted OpenTSDB user. This issue shares the same root cause as CVE-2018-13003, a reflected XSS vulnerability with the suggestion endpoint.	https://githu b.com/Open TSDB/opent sdb/pull/22 74	A-OPE-OPEN- 170523/654
			CVE ID : CVE-2023- 25827		
Vendor: oxi					
Product: acc	sion(s): * Up to (6	excluding	2.3.1		
Improper Neutralizat ion of	04-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS)	N/A	A-OXI-ACCO- 170523/655
CVSS Scoring S	Scale 0-1	1-2 2-3		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')			vulnerability in Biplob Adhikari Accordion – Multiple Accordion or FAQs Builder plugin <= 2.3.0 versions. <b>CVE ID : CVE-2023-</b>		
Vendor nal	letsprojects		25962		
Product: fla					
Affected Ver	sion(s): * Up to (e	excluding)	2.2.5		
Use of Persistent Cookies Containing Sensitive Informatio n	02-May-2023	7.5	Flask is a lightweight WSGI web application framework. When all of the following conditions are met, a response containing data intended for one client may be cached and subsequently sent by the proxy to other clients. If the proxy also caches `Set- Cookie` headers, it may send one client's `session` cookie to other clients. The severity depends on the application's use of the session and the proxy's behavior regarding cookies. The risk depends on all these conditions being met.	https://githu b.com/pallet s/flask/com mit/70f906c 51ce49c485f 1d355703e9 cc3386b1cc2 b, https://githu b.com/pallet s/flask/secu rity/advisori es/GHSA- m2qf-hxjv- 5gpq, https://githu b.com/pallet s/flask/com mit/afd63b1 6170b7c047 f5758eb910c 416511e9c9 65	A-PAL-FLAS- 170523/656

0-1

1-2

**2-3** 3-4 4-5 Page **337** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			strip cookies or ignore responses with cookies.		
			2. The application		
			sets `session.permanent = True`		
			3. The application does not access or modify the session at any point during a request.		
			4. `SESSION_REFRESH_ EACH_REQUEST` enabled (the default).		
			5. The application does not set a `Cache-Control` header to indicate that a page is private or should not be cached.		
			This happens because vulnerable versions of Flask only set the 'Vary: Cookie' header when the session is accessed or modified, not when it is refreshed (re-sent to update the expiration) without being accessed or modified. This issue has been fixed in		
			versions 2.3.2 and 2.2.5.		

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 30861		
Affected Ver	sion(s): From (in	cluding) 2	.3.0 Up to (excluding) 2	.3.2	
Use of Persistent Cookies Containing Sensitive Informatio n	02-May-2023	7.5	Flask is a lightweight WSGI web application framework. When all of the following conditions are met, a response containing data intended for one client may be cached and subsequently sent by the proxy to other clients. If the proxy also caches `Set- Cookie` headers, it may send one client's `session` cookie to other clients. The severity depends on the application's use of the session and the proxy's behavior regarding cookies. The risk depends on all these conditions being met. 1. The application must be hosted behind a caching proxy that does not strip cookies or ignore responses with cookies. 2. The application sets `session.permanent = True`	https://githu b.com/pallet s/flask/com mit/70f906c 51ce49c485f 1d355703e9 cc3386b1cc2 b, https://githu b.com/pallet s/flask/secu rity/advisori es/GHSA- m2qf-hxjv- 5gpq, https://githu b.com/pallet s/flask/com mit/afd63b1 6170b7c047 f5758eb910c 416511e9c9 65	A-PAL-FLAS- 170523/657

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3. The application does not access or modify the session at any point during a request.		
			4. `SESSION_REFRESH_ EACH_REQUEST` enabled (the default).		
			5. The application does not set a `Cache-Control` header to indicate that a page is private or should not be cached.		
			This happens because vulnerable versions of Flask only set the 'Vary: Cookie' header when the session is accessed or modified, not when it is refreshed (re-sent to update the expiration) without		
			being accessed or modified. This issue has been fixed in versions 2.3.2 and 2.2.5.		
			CVE ID : CVE-2023- 30861		
Vendor: pee	epso			l	<u></u>
Product: pe					
	sion(s): * Up to (e	excluding)			
Cross-Site Request	03-May-2023	8.8	Cross-Site Request Forgery (CSRF)	N/A	A-PEE-PEEP- 170523/658
CVSS Scoring S	icale 0-1 1	L-2 2-3	<b>3-4 4-5 5-6</b> Page <b>340</b> of <b>1106</b>	6-7 7-6	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			vulnerability in PeepSo Community by PeepSo plugin <= 6.0.2.0 versions.		
			CVE ID : CVE-2023- 25967		
Vendor: per	freeblog_projec	rt			
Product: pe	rfreeblog				
Affected Ver	sion(s): 3.1.2				
Improper Neutralizat ion of Input During Web Page Generation	01-May-2023	5.4	Cross Site Scripting (XSS) vulnerability in PerfreeBlog 3.1.2 allows attackers to execute arbitrary code via the Post function.	https://githu b.com/perfr ee/PerfreeBl og/issues/1 4	A-PER-PERF- 170523/659
('Cross-site Scripting')			CVE ID : CVE-2023- 29643		
Vendor: Phj	pmyfaq				
Product: ph	pmyfaq				
Affected Ver	sion(s): * Up to (e	excluding)	3.1.13		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	05-May-2023	4.8	Cross-site Scripting (XSS) - Reflected in GitHub repository thorsten/phpmyfaq prior to 3.1.13. <b>CVE ID : CVE-2023-</b> <b>2427</b>	https://githu b.com/thorst en/phpmyfa q/commit/5 14f4df2ad91 8e69575028 d58b2e33aaf 536e59b, https://hunt r.dev/bounti es/89005a6 d-d019- 4cb7-ae88- 486d2d4419 0d	A-PHP-PHPM- 170523/660
Improper Neutralizat ion of Input	05-May-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository	https://githu b.com/thorst en/phpmyfa q/commit/2	A-PHP-PHPM- 170523/661

0-1

1-2

2-33-44-5Page 341 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			thorsten/phpmyfaq prior to 3.1.13. CVE ID : CVE-2023- 2550	0ac51594db 11604a4518 aacc28a51f6 7d4f11bf, https://hunt r.dev/bounti es/840c8d9 1-c97e- 4116-a9f8- 4ab1a38d23 9b	
Vendor: Pin	ncore				
Product: pi					
Affected Ver	sion(s): * Up to (e	excluding)	[		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-May-2023	7.5	Pimcore is an open source data and experience management platform. Versions of Pimcore prior to 10.5.18 are vulnerable to path traversal. The impact of this path traversal and arbitrary extension is limited to creation of arbitrary files and appending data to existing files. When combined with the SQL Injection, the exported data `RESTRICTED DIFFUSION 9 / 9` can be controlled and a webshell can be uploaded. Attackers can use that to execute arbitrary PHP code on the server with the permissions of the	https://githu b.com/pimc ore/pimcore /security/ad visories/GHS A-g2mc- fqqc-hxg3, https://githu b.com/pimc ore/pimcore /commit/f1d 904094700b 513c475690 4fa2b1e19d 08d890e.pat ch, https://githu b.com/pimc ore/pimcore /pull/14498	A-PIM-PIMC- 170523/662

0-1

1-2

2-33-44-5Page 342 of 1106

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webserver. Users may upgrade to version 10.5.18 to receive a patch or, as a workaround, apply the patch manually. <b>CVE ID : CVE-2023-</b> <b>30855</b>		
Affected Ver	sion(s): * Up to (	excluding)	10.5.21	L	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-May-2023	5.4	Cross-site Scripting (XSS) - Generic in GitHub repository pimcore/pimcore prior to 10.5.21. <b>CVE ID : CVE-2023-</b> <b>2616</b>	https://githu b.com/pimc ore/pimcore /commit/07 a2c95be524 c7e20105cef 58c5767d4e bb06091, https://hunt r.dev/bounti es/564cb51 2-2bcc- 4458-8c20- 88110ab458 01	A-PIM-PIMC- 170523/663
Vendor: pix	-				
-	oduct_catalog_fe		244		
Affected Ver Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	sion(s): * Up to (6 02-May-2023	6.1	2.1.1 The Product Catalog Feed by PixelYourSite WordPress plugin before 2.1.1 does not sanitise and escape the edit parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high	N/A	A-PIX-PROD- 170523/664

0-1

1-2

**2-3** 3-4 4-5 Page **343** of **1106**  5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege users such as administrators. CVE ID : CVE-2023- 1804		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	6.1	The Product Catalog Feed by PixelYourSite WordPress plugin before 2.1.1 does not sanitise and escape the page parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin <b>CVE ID : CVE-2023-</b> <b>1805</b>	N/A	A-PIX-PROD- 170523/665
Vendor: plai	inviewplugins			•	
Product: my	vcryptocheckou	t			
Affected Vers	sion(s): * Up to (e	excluding)	2.124	1	1
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	6.1	The MyCryptoCheckout WordPress plugin before 2.124 does not escape some URLs before outputting them in attributes, leading to Reflected Cross-Site Scripting <b>CVE ID : CVE-2023-</b> <b>1546</b>	N/A	A-PLA-MYCR- 170523/666
Vendor: plu	gin-planet				
Product: day	shboard_widget	_suite			
	sion(s): * Up to (e				

0-1

1-2

**2-3** 3-4 4-5 Page **344** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Jeff Starr Dashboard Widgets Suite plugin <= 3.2.1 versions. CVE ID : CVE-2023- 26517	N/A	A-PLU-DASH- 170523/667
Vendor: poo	dofo_project				
Product: po	dofo				
Affected Ver	sion(s): 0.10.0				
Use After Free	10-May-2023	8.8	Podofo v0.10.0 was discovered to contain a heap-use- after-free via the component PoDoFo::PdfEncrypt: :IsMetadataEncrypte d(). <b>CVE ID : CVE-2023- 31566</b>	https://githu b.com/podof o/podofo/iss ues/70	A-POD-PODO- 170523/668
Out-of- bounds Write	10-May-2023	8.8	Podofo v0.10.0 was discovered to contain a heap buffer overflow via the component PoDoFo::PdfEncrypt AESV3::PdfEncryptA ESV3. <b>CVE ID : CVE-2023-</b> <b>31567</b>	https://githu b.com/podof o/podofo/iss ues/71	A-POD-PODO- 170523/669
Out-of- bounds Write	10-May-2023	8.8	Podofo v0.10.0 was discovered to contain a heap buffer overflow via the component PoDoFo::PdfEncrypt RC4::PdfEncryptRC4.	https://githu b.com/podof o/podofo/iss ues/72	A-POD-PODO- 170523/670

0-1

1-2

**2-3** 3-4 4-5 Page **345** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 31568		
Vendor: Poo	lsfoundation				•
Product: po	ds				
Affected Ver	sion(s): * Up to (e	excluding)	2.9.11		
Cross-Site Request Forgery (CSRF)	03-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Pods Framework Team Pods – Custom Content Types and Fields plugin <= 2.9.10.2 versions. <b>CVE ID : CVE-2023-</b>	N/A	A-POD-PODS- 170523/671
Vandamme			23790		
Vendor: pre					
-	emmerce_redir				
Affected Ver	sion(s): * Up to (i	ncluding)		1	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site	10-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Premmerce Premmerce Redirect Manager plugin <= 1.0.9 versions.	N/A	A-PRE-PREM- 170523/672
Scripting')			CVE ID : CVE-2023-		
	-		23789		
Vendor: Pre	_				
Product: pr	-				
Affected Ver	sion(s): 1.7.7.4				
Improper Neutralizat ion of Input During Web Page Generation	11-May-2023	6.1	A cross-site scripting (XSS) vulnerability in PrestaShop v1.7.7.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the	N/A	A-PRE-PRES- 170523/673

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			message parameter in /contactform/contac tform.php. CVE ID : CVE-2023- 31508		
Product: sce	exportcustomer	S			
Affected Vers	sion(s): * Up to (i	ncluding)	3.6.1		
N/A	04-May-2023	7.5	PrestaShop scexportcustomers <= 3.6.1 is vulnerable to Incorrect Access Control. Due to a lack of permissions' control, a guest can access exports from the module which can lead to leak of personal information from customer table. <b>CVE ID : CVE-2023-</b> <b>30282</b>	N/A	A-PRE-SCEX- 170523/674
Vendor: pro	filepress				
Product: pro	ofilepress				
Affected Vers	sion(s): * Up to (e	excluding)	4.5.5		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ProfilePress Membership Team ProfilePress plugin <= 4.5.4 versions. <b>CVE ID : CVE-2023-</b> <b>23830</b>	N/A	A-PRO-PROF- 170523/675
Vendor: pro	perfraction			<u> </u>	I
Product: pro	ofilepress				
Affected Vers	sion(s): * Up to (	excluding)	4.5.5		
Improper Neutralizat	03-May-2023	5.4	Auth. (contributor+) Stored Cross-Site	N/A	A-PRO-PROF- 170523/676
CVSS Scoring S	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
ion of Input During Web Page Generation ('Cross-site			Scripting (XSS) vulnerability in ProfilePress Membership Team ProfilePress plugin <= 4.5.4 versions.		
Scripting')			CVE ID : CVE-2023- 23820		
Vendor: pub	olish_to_schedul	e_project			
Product: pu	blish_to_schedu	le			
Affected Vers	sion(s): * Up to (e	excluding)	4.5.5	-	-
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site	06-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Alex Benfica Publish to Schedule plugin <= 4.5.4 versions. <b>CVE ID : CVE-2023-</b>	N/A	A-PUB-PUBL- 170523/677
Scripting')			26519		
Vendor: Pup	-				
-	<pre>ppet_enterprise sion(s): 2021.7.1</pre>	2			
N/A	04-May-2023	5.3	A Regular Expression Denial of Service (ReDoS) issue was discovered in Puppet Server 7.9.2 certificate validation. An issue related to specifically crafted certificate names significantly slowed down server operations. <b>CVE ID : CVE-2023-</b> <b>1894</b>	https://ww w.puppet.co m/security/ cve/cve- 2023-1894- puppet- server-redos	A-PUP-PUPP- 170523/678
Affected Vers	sion(s): 2023.0				

0-1

1-2

**2-3** 3-4 4-5 Page **348** of **1106**  5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
N/A	04-May-2023	5.3	A Regular Expression Denial of Service (ReDoS) issue was discovered in Puppet Server 7.9.2 certificate validation. An issue related to specifically crafted certificate names significantly slowed down server operations. <b>CVE ID : CVE-2023-</b> <b>1894</b>	https://ww w.puppet.co m/security/ cve/cve- 2023-1894- puppet- server-redos	A-PUP-PUPP- 170523/679		
Product: pu	ppet_server						
Affected Ver	sion(s): 7.9.2						
N/A	04-May-2023	5.3	A Regular Expression Denial of Service (ReDoS) issue was discovered in Puppet Server 7.9.2 certificate validation. An issue related to specifically crafted certificate names significantly slowed down server operations. <b>CVE ID : CVE-2023-</b> <b>1894</b>	https://ww w.puppet.co m/security/ cve/cve- 2023-1894- puppet- server-redos	A-PUP-PUPP- 170523/680		
Vendor: qbi	an61_forum-jav	a_project	t				
Product: qb	ian61_forum-ja	va					
Affected Ver	Affected Version(s): -						
Improper Neutralizat ion of Input During Web Page Generation	01-May-2023	6.1	Cross Site Scripting (XSS) vulnerability in Qbian61 forum-java, allows attackers to inject arbitrary web script or HTML via editing the article	N/A	A-QBI-QBIA- 170523/681		

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			content in the "article editor" page.		
			CVE ID : CVE-2023- 29637		
Vendor: qua	antumcloud				
Product: ai					
Affected Ver	sion(s): * Up to (e	excluding)		I	
Cross-Site Request Forgery (CSRF)	08-May-2023	6.1	The AI ChatBot WordPress plugin before 4.4.5 does not escape most of its settings before outputting them back in the dashboard, and does not have a proper CSRF check, allowing attackers to make a logged in admin set XSS payloads in them. <b>CVE ID : CVE-2023-</b> <b>1011</b>	N/A	A-QUA-AI_C- 170523/682
Affected Ver	sion(s): * Up to (e	excluding)	4.4.7		
Deserializa tion of Untrusted Data	08-May-2023	9.8	The AI ChatBot WordPress plugin before 4.4.7 unserializes user input from cookies via an AJAX action available to unauthenticated users, which could allow them to perform PHP Object Injection when a suitable gadget is present on the blog <b>CVE ID : CVE-2023-</b> <b>1650</b>	N/A	A-QUA-AI_C- 170523/683

0-1

1-2

**2-3** 3-4 4-5 Page **350** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): * Up to (	excluding)	4.4.9	L	1
Cross-Site Request Forgery (CSRF)	08-May-2023	6.1	The AI ChatBot WordPress plugin before 4.4.9 does not have authorisation and CSRF in a function hooked to init, allowing unauthenticated users to update some settings, leading to Stored XSS due to the lack of escaping when outputting them in the admin dashboard <b>CVE ID : CVE-2023-</b>	N/A	A-QUA-AI_C- 170523/684
Cross-Site Request Forgery (CSRF)	08-May-2023	5.4	1660 The AI ChatBot WordPress plugin before 4.4.9 does not have authorisation and CSRF in the AJAX action responsible to update the OpenAI settings, allowing any authenticated users, such as subscriber to update them. Furthermore, due to the lack of escaping of the settings, this could also lead to Stored XSS CVE ID : CVE-2023- 1651	N/A	A-QUA-AI_C- 170523/685
Affected Ver	sion(s): * Up to (e	excluding)	4.5.1		
Improper Neutralizat ion of Input	08-May-2023	4.8	The AI ChatBot WordPress plugin before 4.5.1 does not sanitise and escape	N/A	A-QUA-AI_C- 170523/686

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')			numerous of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) CVE ID : CVE-2023- 1649				
Vendor: red	liker						
Product: ad	minplus						
Affected Ver	sion(s): 6.1.91.00	)					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Cross Site Scripting (XSS) vulnerability in Rediker Software AdminPlus 6.1.91.00 allows remote attackers to run arbitrary code via the onload function within the application DOM. <b>CVE ID : CVE-2023-</b> <b>24744</b>	N/A	A-RED-ADMI- 170523/687		
Vendor: ret	urn_and_warrar	nty_mana	gement_system_for_w	oocommerce_p	project		
Product: ret	turn_and_warra	nty_mana	ngement_system_for_w	voocommerce			
Affected Ver	Affected Version(s): * Up to (including) 1.2.3						
Improper Neutralizat ion of Input During Web Page Generation	08-May-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in chilidevs Return and Warranty Management System for WooCommerce	N/A	A-RET-RETU- 170523/688		

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			plugin <= 1.2.3 versions.		
			CVE ID : CVE-2023- 22710		
Vendor: ros	ariosis				
Product: ro	sariosis				
Affected Ver	sion(s): 10.8.4				
Improper Neutralizat ion of Formula Elements in a CSV File	02-May-2023	5.4	RosarioSIS 10.8.4 is vulnerable to CSV injection via the Periods Module. CVE ID : CVE-2023- 29918	N/A	A-ROS-ROSA- 170523/689
Vendor: S-c	ms				
Product: S-o	cms				
Affected Ver	sion(s): 5.0				
N/A	05-May-2023	7.2	S-CMS v5.0 was discovered to contain an authenticated remote code execution (RCE) vulnerability via the component /admin/ajax.php. CVE ID : CVE-2023- 29963	N/A	A-S-C-S-CM- 170523/690
Vendor: Sar	_				
	msung_blockcha				
Affected Ver	sion(s): * Up to (	excluding)		1	
Out-of- bounds Write	04-May-2023	7.8	Out-of-bounds Write vulnerability while processing BC_TUI_CMD_SEND_ RESOURCE_DATA_A RRAY command in bc_tui trustlet from Samsung Blockchain	https://secu rity.samsung mobile.com/ serviceWeb.s msb?year=2 023&month =05	A-SAM-SAMS- 170523/691

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
			Keystore prior to version 1.3.12.1 allows local attacker to execute arbitrary code.		
			CVE ID : CVE-2023- 21506		
Out-of- bounds Write	04-May-2023	7.8	Out-of-bounds Write vulnerability while processing BC_TUI_CMD_SEND_ RESOURCE_DATA command in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to execute arbitrary code. <b>CVE ID : CVE-2023-</b> <b>21508</b>	https://secu rity.samsung mobile.com/ serviceWeb.s msb?year=2 023&month =05	A-SAM-SAMS- 170523/692
Out-of- bounds Write	04-May-2023	7.8	Out-of-bounds Write vulnerability while processing BC_TUI_CMD_UPDAT E_SCREEN in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to execute arbitrary code. <b>CVE ID : CVE-2023-</b> <b>21509</b>	https://secu rity.samsung mobile.com/ serviceWeb.s msb?year=2 023&month =05	A-SAM-SAMS- 170523/693
Out-of- bounds Read	04-May-2023	5.5	Out-of-bounds Read vulnerability while processing BC_TUI_CMD_SEND_ RESOURCE_DATA_A RRAY command in	https://secu rity.samsung mobile.com/ serviceWeb.s msb?year=2	A-SAM-SAMS- 170523/694

0-1

1-2

**2-3** 3-4 4-5 Page **354** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to read arbitrary memory. <b>CVE ID : CVE-2023-</b>	023&month =05		
Out-of- bounds Read	04-May-2023	5.5	21507 Out-of-bounds Read vulnerability while processing BC_TUI_CMD_UPDAT E_SCREEN in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to read arbitrary memory. CVE ID : CVE-2023- 21510	https://secu rity.samsung mobile.com/ serviceWeb.s msb?year=2 023&month =05	A-SAM-SAMS- 170523/695	
Out-of- bounds Read	04-May-2023	5.5	Out-of-bounds Read vulnerability while processing CMD_COLDWALLET_ BTC_SET_PRV_UTXO in bc_core trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to read arbitrary memory. <b>CVE ID : CVE-2023-</b> <b>21511</b>	https://secu rity.samsung mobile.com/ serviceWeb.s msb?year=2 023&month =05	A-SAM-SAMS- 170523/696	
Product: samsung_core_services						
Affected Vers	sion(s): * Up to (e	excluding)	2.1.00.36			
N/A	04-May-2023	8.6	Improper access control in Samsung	https://secu rity.samsung	A-SAM-SAMS- 170523/697	
CVSS Scoring S	Scale 0-1 2	1-2 2-3	<b>3-4 4-5 5-6</b>	6-7 7-8	8 8-9 9-10	

**2-3** 3-4 4-5 Page **355** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			Core Service prior to version 2.1.00.36 allows attacker to write arbitrary file in sandbox.	mobile.com/ serviceWeb.s msb?year=2 023&month =05		
			CVE ID : CVE-2023- 21505			
Vendor: san	dhillsdev					
Product: ea	sy_digital_down	loads				
Affected Ver	sion(s): From (in	cluding) 3	.1 Up to (excluding) 3.1	.1.4.2		
Improper Authentica tion	02-May-2023	9.8	Improper Authentication vulnerability in Easy Digital Downloads plugin allows unauth. Privilege Escalation. This issue affects Easy Digital Downloads: from 3.1 through 3.1.1.4.1. <b>CVE ID : CVE-2023-</b> <b>30869</b>	https://patc hstack.com/ articles/criti cal-easy- digital- downloads- vulnerability ?_s_id=cve	A-SAN-EASY- 170523/698	
Vendor: SAI	<b>P</b>				I	
Product: bu	sinessobjects					
Affected Ver	sion(s): 4.20					
Insufficient ly Protected Credentials	09-May-2023	5.9	SAP BusinessObjects Platform - versions 420, 430, Information design tool transmits sensitive information as cleartext in the binaries over the network. This could allow an unauthenticated attacker with deep knowledge to gain sensitive information such as user credentials and	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-BUSI- 170523/699	
credentials and						

Page **356** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			domain names, which may have a low impact on confidentiality and no impact on the integrity and availability of the system.		
			CVE ID : CVE-2023- 28764		
Affected Ver	sion(s): 4.30				
Insufficient ly Protected Credentials	09-May-2023	5.9	SAP BusinessObjects Platform - versions 420, 430, Information design tool transmits sensitive information as cleartext in the binaries over the network. This could allow an unauthenticated attacker with deep knowledge to gain sensitive information such as user credentials and domain names, which may have a low impact on confidentiality and no impact on the integrity and availability of the system. CVE ID : CVE-2023- 28764	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-BUSI- 170523/700

0-1

1-2

**2-3** 3-4 4-5 Page **357** of **1106**  5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: bu	sinessobjects_b	usiness_i	ntelligence		
Affected Ver	sion(s): 420				
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	09-May-2023	7.6	SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an authenticated attacker to access sensitive information which is otherwise restricted. On successful exploitation, there could be a high impact on confidentiality, limited impact on integrity and availability of the application. CVE ID : CVE-2023- 30740	https://laun chpad.suppo rt.sap.com/# /notes/3313 484, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-BUSI- 170523/701
N/A	09-May-2023	7.2	SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an authenticated attacker with administrator privileges to get the login token of any logged-in BI user over the network without any user interaction. The attacker can impersonate any user on the platform resulting into accessing and	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-BUSI- 170523/702

0-1

1-2

**2-3** 3-4 4-5 Page **358** of **1106**  7-8

6-7

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying data. The attacker can also make the system partially or entirely unavailable.		
			CVE ID : CVE-2023- 28762		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to insufficient input validation, SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an unauthenticated attacker to redirect users to untrusted site using a malicious link. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application.	https://laun chpad.suppo rt.sap.com/# /notes/3309 935, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-BUSI- 170523/703
			CVE ID : CVE-2023- 30741		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to insufficient input validation, SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an unauthenticated attacker to redirect users to untrusted	https://laun chpad.suppo rt.sap.com/# /notes/3319 400, https://ww w.sap.com/d ocuments/2 022/02/fa86	A-SAP-BUSI- 170523/704

0-1

1-2

**2-3** 3-4 4-5 Page **359** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			site using a malicious link. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application.	5ea4-167e- 0010-bca6- c68f7e60039 b.html	
			CVE ID : CVE-2023- 31406		
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	09-May-2023	5	Under certain conditions, SAP BusinessObjects Business Intelligence Platform (Central Management Service) - versions 420, 430, allows an attacker to access information which would otherwise be restricted. Some users with specific privileges could have access to credentials of other users. It could let them access data sources which would otherwise be restricted.	https://laun chpad.suppo rt.sap.com/# /notes/3038 911, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-BUSI- 170523/705
Affected Version(s): 430					
Exposure of Sensitive	09-May-2023	7.6	SAP BusinessObjects Business Intelligence	https://laun chpad.suppo	A-SAP-BUSI- 170523/706
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10           Page 360 of 1106					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Informatio n to an Unauthoriz ed Actor			Platform - versions 420, 430, allows an authenticated attacker to access sensitive information which is otherwise restricted. On successful exploitation, there could be a high impact on confidentiality, limited impact on integrity and availability of the application.	rt.sap.com/# /notes/3313 484, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	
			<b>CVE ID : CVE-2023-</b> <b>30740</b> SAP BusinessObjects		
N/A	09-May-2023	7.2	SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an authenticated attacker with administrator privileges to get the login token of any logged-in BI user over the network without any user interaction. The attacker can impersonate any user on the platform resulting into accessing and modifying data. The attacker can also make the system	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-BUSI- 170523/707

0-1

1-2

2-33-44-5Page 361 of 1106

6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			partially or entirely unavailable. <b>CVE ID : CVE-2023-</b>		
			28762		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to insufficient input validation, SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an unauthenticated attacker to redirect users to untrusted site using a malicious link. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application.	https://laun chpad.suppo rt.sap.com/# /notes/3309 935, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-BUSI- 170523/708
			CVE ID : CVE-2023- 30741		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to insufficient input validation, SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an unauthenticated attacker to redirect users to untrusted site using a malicious link. On successful exploitation, an	https://laun chpad.suppo rt.sap.com/# /notes/3319 400, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6-	A-SAP-BUSI- 170523/709

0-1

1-2

2-33-44-5Page 362 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			attacker can view or modify information causing a limited impact on confidentiality and integrity of the application. <b>CVE ID : CVE-2023-</b> <b>31406</b>	c68f7e60039 b.html			
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	09-May-2023	5	Under certain conditions, SAP BusinessObjects Business Intelligence Platform (Central Management Service) - versions 420, 430, allows an attacker to access information which would otherwise be restricted. Some users with specific privileges could have access to credentials of other users. It could let them access data sources which would otherwise be restricted.	https://laun chpad.suppo rt.sap.com/# /notes/3038 911, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-BUSI- 170523/710		
_			31404				
Product: business_planning_and_consolidation Affected Version(s): 740							
			CAD Ducines	https://l-			
Improper Neutralizat ion of	09-May-2023	5.4	SAP Business Planning and Consolidation -	https://laun chpad.suppo rt.sap.com/#	A-SAP-BUSI- 170523/711		
Input			versions 740, 750,	/notes/3312			
CVSS Scoring S	Scale 0-1 3	1-2 2-3			8 8-9 9-10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
During Web Page Generation ('Cross-site Scripting')			allows an authorized attacker to upload a malicious file, resulting in Cross- Site Scripting vulnerability. After successful exploitation, an attacker can cause limited impact on confidentiality and integrity of the application.	892, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html			
Affected Vers	sion(s): 750		CVE ID : CVE-2023- 31407				
			SAP Business				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Planning and Consolidation - versions 740, 750, allows an authorized attacker to upload a malicious file, resulting in Cross- Site Scripting vulnerability. After successful exploitation, an attacker can cause limited impact on confidentiality and integrity of the application.	https://laun chpad.suppo rt.sap.com/# /notes/3312 892, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-BUSI- 170523/712		
Duradurui		-hi	CVE ID : CVE-2023- 31407				
Product: cu	Product: customer_relationship_management_s4fnd						

0-1

1-2

**2-3** 3-4 4-5 Page **364** of **1106**  5-6

6-7

7-8 8-9

Affected Version(s): 102       SAP CRM (WebClient UI) - versions S4FND 103, S4FND 103, S4FND 103, S4FND 104, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 700, WEBCUIF 747, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 800, WEB	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation (Cross-stie)09-May-20236.1UI) - versions S4FND 102, S4FND 106, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 747, WEBCUIF 747, WEBCUIF 748, WEBCUIF 748, WEBCUIF 748, WEBCUIF 800, WEBCUIF 800, WEBCUIF 800, WEBCUIF 800, WEBCUIF 801, does not sufficiently controlled inputs, resulting in a stored (Cross-stie Scripting)https://laun https://laun ocuments/2 971, https://ww wsap.com/# ocuments/2 022/02/1866 b.htmlhttps://laun https://laun https://ww wsap.com/#Improper Neutralization of Input During Web Page Generation (Cross-stie Scripting)09-May-20236.1Sap-cust- cost-stie Scripting) b.htmlA-SAP-CUST- to523/713Marker to execute in the victim to click, causing the articker could store script supplied by the attacker to execute in the victim user's session could then be modified or read by the attacker.A-SAP-CUST- to523/713Affected Versures: Improper09-May-20236.1SAP CRM (WebClient bAP CRM The start or b.htmlA-SAP-CUST- to523/713	Affected Vers	sion(s): 102	1			l
Improper     09-May-2023     6.1     SAP CRM (WebClient     https://laun     A-SAP-CUST-	Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')		6.1	UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 747, WEBCUIF 748, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker.	chpad.suppo rt.sap.com/# /notes/3315 971, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039	
09-May-2023 6.1 511 511 511 (Webshenr heps// henr	Affected Vers	sion(s): 103				
		09-May-2023	6.1	•		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 701, WEBCUIF 746, WEBCUIF 746, WEBCUIF 748, WEBCUIF 800, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker.	rt.sap.com/# /notes/3315 971, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	
			CVE ID : CVE-2023- 30742		
Affected Vers	sion(s): 104				
Improper Neutralizat ion of Input During	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106,	https://laun chpad.suppo rt.sap.com/# /notes/3315 971,	A-SAP-CUST- 170523/715

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker.	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	
Affected Ver	sion(s): 105			I	
Improper Neutralizat ion of Input During Web Page Generation	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701,	https://laun chpad.suppo rt.sap.com/# /notes/3315 971, https://ww w.sap.com/d ocuments/2	A-SAP-CUST- 170523/716

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker.	022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	
			CVE ID : CVE-2023- 30742		
Affected Ver	sion(s): 106				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747,	https://laun chpad.suppo rt.sap.com/# /notes/3315 971, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6-	A-SAP-CUST- 170523/717

0-1

1-2

**2-3** 3-4 4-5 Page **368** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker.	c68f7e60039 b.html	
			30742		
Affected Vers	sion(s): 107				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does	https://laun chpad.suppo rt.sap.com/# /notes/3315 971, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-CUST- 170523/718

0-1

1-2

**2-3** 3-4 4-5 Page **369** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not sufficiently encode user- controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker.		
D L t		<b>.</b>	30742	•	
Affected Ver		ship_mar	nagement_webclient_u	1	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 701, WEBCUIF 746, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-CUST- 170523/719

0-1

1-2

**2-3** 3-4 4-5 Page **370** of **1106**  5-6

7-8

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controlled inputs, resulting in Cross- Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data.		
			CVE ID : CVE-2023- 29188		
Affected Ver	sion(s): 7.31				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 701, WEBCUIF 746, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in Cross- Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-CUST- 170523/720

0-1

1-2

2-33-44-5Page 371 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			sensitive information but cannot delete the data.					
			CVE ID : CVE-2023- 29188					
Affected Version(s): 7.46								
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in Cross- Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. <b>CVE ID : CVE-2023- 29188</b>	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-CUST- 170523/721			
Affected Vers	sion(s): 7.47							
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 372 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 746, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in Cross- Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. CVE ID : CVE-2023- 29188	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-CUST- 170523/722
Affected Ver	sion(s): 7.48			<u> </u>	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731,	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-CUST- 170523/723

0-1

1-2

2-33-44-5Page 373 of 1106

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in Cross- Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data.		
			CVE ID : CVE-2023- 29188		
Affected Ver	sion(s): 700				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 701, WEBCUIF 747, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in a stored	https://laun chpad.suppo rt.sap.com/# /notes/3315 971, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-CUST- 170523/724

0-1

1-2

**2-3** 3-4 4-5 Page **374** of **1106**  5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker.		
Affected Ver	sion(s): 701		CVE ID : CVE-2023- 30742		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 701, WEBCUIF 746, WEBCUIF 746, WEBCUIF 746, WEBCUIF 748, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An	https://laun chpad.suppo rt.sap.com/# /notes/3315 971, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-CUST- 170523/725

0-1

1-2

2-33-44-5Page 375 of 1106

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker.		
Affected Ver	sion(s): 731		CVE ID : CVE-2023- 30742		
			SAP CRM (WebClient		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 746, WEBCUIF 748, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to	https://laun chpad.suppo rt.sap.com/# /notes/3315 971, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-CUST- 170523/726

0-1

1-2

**2-3** 3-4 4-5 Page **376** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker. CVE ID : CVE-2023- 30742		
Affected Ver	sion(s): 746				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to	https://laun chpad.suppo rt.sap.com/# /notes/3315 971, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-CUST- 170523/727

0-1

1-2

**2-3** 3-4 4-5 Page **377** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker.		
			CVE ID : CVE-2023- 30742		
Affected Ver	sion(s): 747			1	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the	https://laun chpad.suppo rt.sap.com/# /notes/3315 971, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-CUST- 170523/728

0-1

1-2

**2-3** 3-4 4-5 Page **378** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's session could then be modified or read by the attacker.		
			CVE ID : CVE-2023- 30742		
Affected Ver	sion(s): 748				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be	https://laun chpad.suppo rt.sap.com/# /notes/3315 971, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-CUST- 170523/729

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modified or read by the attacker.		
			CVE ID : CVE-2023- 30742		
Affected Vers	sion(s): 8.00				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 746, WEBCUIF 746, WEBCUIF 748, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in Cross- Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. CVE ID : CVE-2023- 29188	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-CUST- 170523/730

0-1

1-2

**2-3** 3-4 4-5 Page **380** of **1106**  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')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 746, WEBCUIF 748, WEBCUIF 800, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in Cross- Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. CVE ID : CVE-2023- 29188	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-CUST- 170523/731
Affected Ver	sion(s): 800				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731,	https://laun chpad.suppo rt.sap.com/# /notes/3315 971, https://ww w.sap.com/d ocuments/2 022/02/fa86	A-SAP-CUST- 170523/732

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker.	5ea4-167e- 0010-bca6- c68f7e60039 b.html	
Affected Vers	sion(s): 801			I	L
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748,	https://laun chpad.suppo rt.sap.com/# /notes/3315 971, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6-	A-SAP-CUST- 170523/733

0-1

1-2

**2-3** 3-4 4-5 Page **382** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker.	c68f7e60039 b.html	
Product: gu	i_for_windows			I	
Affected Ver	sion(s): 8.0				
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	09-May-2023	9.3	SAP GUI for Windows - version 7.70, 8.0, allows an unauthorized attacker to gain NTLM authentication information of a victim by tricking it into clicking a prepared shortcut file. Depending on the authorizations of the victim, the attacker can read	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html, https://laun chpad.suppo rt.sap.com/# /notes/3320 467	A-SAP-GUI 170523/734

0-1

1-2

**2-3** 3-4 4-5 Page **383** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and modify potentially sensitive information after successful exploitation.		
Affected Ver	sion(s): 7.70		CVE ID : CVE-2023- 32113		
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	09-May-2023	9.3	SAP GUI for Windows - version 7.70, 8.0, allows an unauthorized attacker to gain NTLM authentication information of a victim by tricking it into clicking a prepared shortcut file. Depending on the authorizations of the victim, the attacker can read and modify potentially sensitive information after successful exploitation.	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html, https://laun chpad.suppo rt.sap.com/# /notes/3320 467	A-SAP-GUI 170523/735
Product: ne	tweaver_application	ation_serv	32113 ver_for_java		
Affected Ver	sion(s): 7.50				
Missing Authentica tion for Critical	09-May-2023	9.1	In SAP AS NetWeaver JAVA - versions SERVERCORE 7.50, J2EE-FRMW 7.50,	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e-	A-SAP-NETW- 170523/736

Page 384 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CORE-TOOLS 7.50, an unauthenticated attacker can attach to an open interface and make use of an open naming and directory API to instantiate an object which has methods which can be called without further authorization and authentication. A subsequent call to one of these methods can read or change the state of existing services without any effect on availability.	0010-bca6- c68f7e60039 b.html	
			CVE ID : CVE-2023- 30744		
-	werdesigner_pr	oxy			
Allected ver			In SAP		
Out-of- bounds Write	09-May-2023	7.5	PowerDesigner (Proxy) - version 16.7, an attacker can send a crafted request from a remote host to the proxy machine and crash the proxy server, due to faulty implementation of memory management causing a memory corruption. This leads to a high impact on	https://laun chpad.suppo rt.sap.com/# /notes/3300 624, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-POWE- 170523/737

0-1

1-2

**2-3** 3-4 4-5 Page **385** of **1106**  5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability of the application.		
			CVE ID : CVE-2023- 32111		
Product: s4					
Affected Ver	sion(s): 100			Γ	1
Missing Authorizati on	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 616, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system.	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-S4CO- 170523/738
			CVE ID : CVE-2023- 32112		
Product: s4	fnd				
Affected Ver	sion(s): 102				
Improper Neutralizat	09-May-2023	5.4	SAP CRM WebClient UI - versions	https://ww w.sap.com/d	A-SAP-S4FN- 170523/739
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>386</b> of <b>1106</b>	6-7 7-8	3 8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 746, WEBCUIF 748, WEBCUIF 800, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in Cross- Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. <b>CVE ID : CVE-2023- 29188</b>	ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	
Affected Ver	sion(s): 103				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747,	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-S4FN- 170523/740

0-1

1-2

**2-3** 3-4 4-5 Page **387** of **1106**  5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in Cross- Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data.		
			CVE ID : CVE-2023- 29188		
Affected Ver	sion(s): 104				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 701, WEBCUIF 746, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in Cross- Site Scripting (XSS) vulnerability. After	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-S4FN- 170523/741

0-1

1-2

**2-3** 3-4 4-5 Page **388** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data.		
			CVE ID : CVE-2023- 29188		
Affected Ver	sion(s): 105				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 701, WEBCUIF 746, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in Cross- Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data.	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-S4FN- 170523/742

0-1

1-2

**2-3** 3-4 4-5 Page **389** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2023- 29188					
Affected Vers	sion(s): 106							
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in Cross- Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. <b>CVE ID : CVE-2023- 29188</b>	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-S4FN- 170523/743			
Affected Ver	Affected Version(s): 107							
Improper Neutralizat ion of Input	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND	https://ww w.sap.com/d ocuments/2 022/02/fa86	A-SAP-S4FN- 170523/744			

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')			103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 746, WEBCUIF 747, WEBCUIF 800, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in Cross- Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data.	5ea4-167e- 0010-bca6- c68f7e60039 b.html	
			CVE ID : CVE-2023- 29188		
Affected Ver	sion(s): 1.02				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800,	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-S4FN- 170523/745

0-1

1-2

2-33-44-5Page 391 of 1106

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in Cross- Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data.		
			CVE ID : CVE-2023- 29188		
Product: say					
Allected Ver			SAP CRM WebClient		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 701, WEBCUIF 746, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user- controlled inputs, resulting in Cross- Site Scripting (XSS) vulnerability. After successful	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-SAPS- 170523/746

0-1

1-2

2-33-44-5Page 392 of 1106

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data.		
Product: say			CVE ID : CVE-2023- 29188		
			Due to improper		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	neutralization of input in SAPUI5 - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200, sap.m.FormattedText SAPUI5 control allows injection of untrusted CSS. This blocks user's interaction with the application. Further, in the absence of URL validation by the application, the vulnerability could lead to the attacker reading or modifying user's information through phishing attack.	https://laun chpad.suppo rt.sap.com/# /notes/3326 210, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-SAPU- 170523/747
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 **393** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 700				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to improper neutralization of input in SAPUI5 - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200, sap.m.FormattedText SAPUI5 control allows injection of untrusted CSS. This blocks user's interaction with the application. Further, in the absence of URL validation by the application, the vulnerability could lead to the attacker reading or modifying user's information through phishing attack.	https://laun chpad.suppo rt.sap.com/# /notes/3326 210, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-SAPU- 170523/748
Affected Ver	sion(s): 754			L	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to improper neutralization of input in SAPUI5 - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200, sap.m.FormattedText SAPUI5 control allows injection of untrusted CSS. This	https://laun chpad.suppo rt.sap.com/# /notes/3326 210, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6-	A-SAP-SAPU- 170523/749

0-1

1-2

**2-3** 3-4 4-5 Page **394** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			blocks user's interaction with the application. Further, in the absence of URL validation by the application, the vulnerability could lead to the attacker reading or modifying user's information through phishing attack.	c68f7e60039 b.html	
			CVE ID : CVE-2023- 30743		
Affected Ver	sion(s): 755				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to improper neutralization of input in SAPUI5 - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200, sap.m.FormattedText SAPUI5 control allows injection of untrusted CSS. This blocks user's interaction with the application. Further, in the absence of URL validation by the application, the vulnerability could lead to the attacker reading or modifying user's information through phishing attack.	https://laun chpad.suppo rt.sap.com/# /notes/3326 210, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-SAPU- 170523/750

0-1

1-2

**2-3** 3-4 4-5 Page **395** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 30743		
Affected Ver	sion(s): 756				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to improper neutralization of input in SAPUI5 - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200, sap.m.FormattedText SAPUI5 control allows injection of untrusted CSS. This blocks user's interaction with the application. Further, in the absence of URL validation by the application, the vulnerability could lead to the attacker reading or modifying user's information through phishing attack.	https://laun chpad.suppo rt.sap.com/# /notes/3326 210, https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-SAPU- 170523/751
Affected Ver	sion(s): 757				
Improper Neutralizat ion of Input During Web Page Generation	09-May-2023	6.1	Due to improper neutralization of input in SAPUI5 - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200,	https://laun chpad.suppo rt.sap.com/# /notes/3326 210, https://ww w.sap.com/d ocuments/2	A-SAP-SAPU- 170523/752

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			sap.m.FormattedText SAPUI5 control allows injection of untrusted CSS. This blocks user's interaction with the application. Further, in the absence of URL validation by the application, the vulnerability could lead to the attacker reading or modifying user's information through phishing attack.	022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	
Product: ve	ndor_master_hi	erarchy	CVE ID : CVE-2023- 30743		
	sion(s): sap_appl				
Missing Authorizati on	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-VEND- 170523/753

0-1

1-2

**2-3** 3-4 4-5 Page **397** of **1106**  5-6

6-7

7-8 8-9

Missing Authorizatio09-May-20235.5Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 603, SAP_APPL 604, SAP_APPL 606, SAP_APPL 606, SAP_APPL 617, SAP_APPL 616, SAP_APPL 617, SAP_APPL 617, SAP_APPL 617, SAP_APPL 618, S4OCRE 100, does not perform necessary authorizatio checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system.https://ww wsap.com/d ocuments/2 022/02/fa86 ASAP-XPU.Missing Authorizatio09-May-20235.5Vendor Master Hierarchy - versions SAP_APPL 606, SAP_APPL 606, SAP_APPL 617, SAP_APPL 617, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system.A-SAP-VEND- 170523/754	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Image: Market Signer				impacting the integrity of the		
Missing Authorizati on09-May-20235.5Vendor Master Hierarchy - versions SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 605, SAP_APPL 605, SAP_APPL 616, SAP_APPL 616, SAP_APPL 616, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system.https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 010-bca6- c687/e60039 b.htmlA-SAP-VEND- 170523/754	Affected Ver	sion(c); can appl	600			
Missing Authorizati on09-May-20235.5File Hierarchy - versions SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 606, SAP_APPL 616, SAP_APPL 616, SAP_APPL 616, SAP_APPL 618, SAP_APPL 618, SAP_APPL 618, SAP_APPL 618, SAP_APPL 618, SAP_APPL 618, SAP_APPL 618, SAP_APPL 618, SAP_APPL 618, SAP_APPL 616, SAP_APPL 616, SAP_APPL 616, SAP_APPL 616, SAP_APPL 616, SAP_APPL 616, SAP_APPL 616, SAP_APPL 618, SAP_APPL 618, SAP_APPL 618, SAP_APPL 618, SAP_APPL 616, SAP_APPL 618, SAP_APPL 618, SAP_APPL 616, SAP_APPL 616, <td>Allected ver</td> <td>sion(s): sap_appi</td> <td>_000</td> <td>Vendor Master</td> <td></td> <td></td>	Allected ver	sion(s): sap_appi	_000	Vendor Master		
52112	Authorizati	09-May-2023	5.5	Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system.	w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039	

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorizati on	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system. <b>CVE ID : CVE-2023- 32112</b>	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-VEND- 170523/755
Affected Ver	sion(s): sap_appl	603			
Missing Authorizati on	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-VEND- 170523/756

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system.		
			CVE ID : CVE-2023- 32112		
Affected Ver	sion(s): sap_appl	_604			
Missing Authorizati on	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 616, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system.	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-VEND- 170523/757

0-1

1-2

**2-3** 3-4 4-5 Page **400** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2023- 32112					
Affected Ver	sion(s): sap_appl	_605						
Missing Authorizati on	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 616, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system.	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-VEND- 170523/758			
			CVE ID : CVE-2023- 32112					
Affected Ver	Affected Version(s): sap_appl_606							
Missing Authorizati on	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605,	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-VEND- 170523/759			

0-1

1-2

**2-3** 3-4 4-5 Page **401** of **1106** 

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system.		
			CVE ID : CVE-2023- 32112		
Affected Ver	sion(s): sap_appl	_616			
Missing Authorizati on	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-VEND- 170523/760

0-1

1-2

**2-3** 3-4 4-5 Page **402** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacting the integrity of the system.		
			CVE ID : CVE-2023- 32112		
Affected Vers	sion(s): sap_appl	_617			
Missing Authorizati on	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system. <b>CVE ID : CVE-2023- 32112</b>	https://ww w.sap.com/d ocuments/2 022/02/fa86 5ea4-167e- 0010-bca6- c68f7e60039 b.html	A-SAP-VEND- 170523/761
Affected Vers	sion(s): sap_appl	_618			
Missing Authorizati on	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600,	https://ww w.sap.com/d ocuments/2 022/02/fa86	A-SAP-VEND- 170523/762
CVSS Scoring S	Scale 0-1 1	1-2 2-3	3-4 4-5 5-6 Page <b>403</b> of <b>1106</b>	6-7 7-8	8 8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system. CVE ID : CVE-2023- 32112	5ea4-167e- 0010-bca6- c68f7e60039 b.html	
Vendor: sca	nservjs_project				
Product: sca	anservjs				
Affected Ver	sion(s): * Up to (e	excluding)	2.27.0		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	07-May-2023	10	OS Command Injection in GitHub repository sbs20/scanservjs prior to v2.27.0. <b>CVE ID : CVE-2023- 2564</b>	https://githu b.com/sbs20 /scanservjs/ commit/d51 fd52c15698 13990b8f74 e64ae6979c 665dca1, https://hunt r.dev/bounti es/d13113a d-a107- 416b-acc1-	A-SCA-SCAN- 170523/763

0-1

1-2

**2-3** 3-4 4-5 Page **404** of **1106**  5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				01e4c16ec4 61				
Vendor: Sen	n-cms				<u> </u>			
Product: Se	mcms							
Affected Ver	sion(s): 4.2							
Unrestricte d Upload of File with Dangerous Type	05-May-2023	9.8	Semcms Shop v4.2 was discovered to contain an arbitrary file uplaod vulnerability via the component SEMCMS_Upfile.php. This vulnerability allows attackers to execute arbitrary code via uploading a crafted PHP file.	N/A	A-SEM-SEMC- 170523/764			
			CVE ID : CVE-2023- 30090					
Vendor: seo	-							
Product: see								
Affected Ver	sion(s): * Up to (e	excluding)	6.5.0.3 The SEOPress	1	1			
Deserializa tion of Untrusted Data	tion of Untrusted Data 02-May-2023 7.2 could allow high- privilege users such as admin to perform PHP Object Injection when a suitable gadget is present. <b>CVE ID : CVE-2023-</b> 1669							
	Vendor: simple_portfolio_gallery_project							
	nple_portfolio_g	allery						
Affected Ver	sion(s): 0.1							

0-1

1-2

**2-3** 3-4 4-5 Page **405** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Tauhidul Alam Simple Portfolio Gallery plugin <= 0.1 versions. <b>CVE ID : CVE-2023-</b> <b>26016</b>	N/A	A-SIM-SIMP- 170523/766
Vendor: sim	ple_youtube_re	sponsive	_project		
Product: sin	nple_youtube_ro	esponsive	9		
Affected Ver	sion(s): * Up to (e	excluding)	3.0		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Eirudo Simple YouTube Responsive plugin <= 2.5 versions. CVE ID : CVE-2023- 25982	N/A	A-SIM-SIMP- 170523/767
Vendor: slo	th_logo_customi	zer_proje	ect		
Product: slo	oth_logo_custom	izer			
Affected Ver	sion(s): * Up to (i	ncluding)	2.0.2		
Cross-Site Request Forgery (CSRF)	08-May-2023	8.8	The Sloth Logo Customizer WordPress plugin through 2.0.2 does not have CSRF check when updating its settings, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	N/A	A-SLO-SLOT- 170523/768

0-1

1-2

**2-3** 3-4 4-5 Page **406** of **1106**  5-6

6-7

8-9

9-10

Vendor: smt-j-mailing_queu-projectCVE ID : CVE-2023- 0603IndexIndexProduct: smt-j-mailing_queu-projectAffected Verson(s): * Up to (excluding 2 0.1)Affected Verson(s): * Up to (excluding 2 0.1)Affected Verson(s): * Up to (excluding 2 0.1)Affected Verson(s): * Up to (excluding 2 0.1)Queue WordPress plugin before 2.0.1Affected Verson(s): * Up to (excluding 2 0.1)Operating the 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)Verdor: sockVerdor: sockCVE ID : CVE-2023- 1090Affected Verson(s): From (including) 5-1.0 Up to (excluding) 6-1.0 transport-based (cross-site Scripting)Affected Verson(s): From (including) 5-1.0 Up to (excluding) 6-1.0 transport-based (cross-site Scripting)Affected Verson(s): From (including) 5-1.0 Up to (excluding) 6-1.0 transport-based (cross-site Scripting)N/A08-May-20236.5Engine.10 is the implementation of transport-based (cross) (crosmin (fr4 80b41305c1 665972763 72dc44, https://githu b.com/socke tio/engineio /2dc44, https://githu b.com/socke tio/engineio /security/ad yeisen 5.1.0 and included in version version 5.1.0 and included in version yeisen 5.1.0 and included in version yeisen 5.1.0 and yeisen 5.1.0 and yeisen 5.1.0 and included in version yeisen 5.1.0 and yeisen 5.1.0 and yeisen 5.1.0 and<	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: smtp_mailing_queueAffected Version(s): * Up to (excluding) 2.0.1Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')The SMTP Mailing Queue WordPress plugin before 2.0.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)N/AA-SMT-SMTP- 170523/769Vendor: socketVerifice (for example in multisite setup)N/AA-SMT-SMTP- 170523/769Vendor: socketProduct: engine.ioAffected Version(s): From (including) 5.1.0 Up to (excluding) 6.4.2N/A08-May-20236.5Engine.I0 is the implementation of transport-based cross- device bi-directional communication layer for Socket 10. An unaraght exception vulnerability was introduced in version 5.1.0 and included in version for Socket 10. An unaraght exception vulnerability was introduced in version for Socket 10. An unaraght exception visories/GHS A-9mw-A-SOC-ENGI- 70523/770						
Affected Version(s): * Up to (excluding) 2.0.1Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')The SMTP Mailing Queue WordPress plugin before 2.0.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) CVE ID : CVE-2023- 1090N/AA-SMT-SMTP- 170523/769Vendor: socketEngine.10 is the implementation of transport-based cross- device bi-directional communication layer for Socket.IO. An uncanght exception vuncarability was htmachanic in reduction layer for Socket.IO. An uncanght exception version 5.1.0 and introduced in version 5.1.0 and visories/GHS A-09mw-A-SOC-ENGI- 70523/770N/A08-May-20236.5Engine.10 is the implementation of transport-based cross- device bi-directional communication layer for Socket.IO. An uncanght exception visories/GHS A-09mw-https://githu b.com/socke tio/engine.io /socke for Socket.IO. An uncanght exception visories/GHS A-09mw-A-SOC-ENGI- 70523/770	Vendor: sm	tp_mailing_queu	ie_projec	t		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')02-May-20234.8The SMTP Mailing Queue WordPress plugin before 2.0.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)N/AA-SMT-SMTP- 170523/769Verden: SocketVerden: SocketProduct: engine.ioAffected Version(s): From (including) 5.1.0 Up to (excluding) 6.4.2Affected Version(s): From (including) 5.1.0 Up to (excluding) 6.4.2N/A08-May-20236.5Engine.IO is the implementation of transport-based cross- device bi-directional communication layer for SocketI.0.An uncaught exception https://githu b.com/socke tio/engine.io /commit/fc44, https://githu b.com/socke tio/engine.io /2055e5983 72dc44, https://githu b.com/socke tio/engine.io /20523/770N/A08-May-20236.5Engine.IO is the inplementation of transport-based cross- device bi-directional communication layer for SocketI.0.An uncaught exception introduced in version 5.1.0 and visories/GHIS A-g9mw-A-SOC-ENGI- 70523/770	Product: sn	ntp_mailing_que	ue			
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')02-May-2023 4.84.8Queue WordPress plugin before 2.0.1 does not sanitise and 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/AA-SMT-SMTP- 170523/769Vendor: sock-Vertice verticeVertice verticeVertice verticeA-SMT-SMTP- 170523/769Vendor: sock-Vertice verticeVertice verticeVertice verticeA-SMT-SMTP- 170523/769VerticeVertice verticeVertice verticeVertice verticeA-SMT-SMTP- 170523/769VerticeVertice verticeVertice verticeVertice verticeA-SMT-SMTP- 170523/769VerticeVertice verticeVertice verticeN/AA-SMT-SMTP- 170523/769N/A08-May-20236.5Engine.10 is the implementation of vertice b-directional communication layer for Socket 10.4 vunerability was introduced in version 5.10 and incuded in version version 5.10 and version 5.10 and	Affected Ver	sion(s): * Up to (	excluding)	2.0.1		
Vendor: socketProduct: engine.ioAffected Version(s): From (including) 5.1.0 Up to (excluding) 6.4.2Affected Version(s): From (including) 5.1.0 Up to (excluding) 6.4.2N/ARay-202308-May-20236.56.5Engine.IO is the implementation of cross- device bi-directional communication layer for Socket.IO. An uncaught exception vulnerability was introduced in version 5.1.0 and included in version 5.1.0 and included in version 4.1.0 of the	Neutralizat ion of Input During Web Page Generation ('Cross-site	02-May-2023	4.8	Queue WordPress plugin before 2.0.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	N/A	
Product: engine.ioAffected Version(s): From (including) 5.1.0 Up to (excluding) 6.4.2Affected Version(s): From (including) 5.1.0 Up to (excluding) 6.4.2https://githuimplementation of transport-basedhttps://githuimplementation of transport-basedb.com/socketransport-basedtio/engine.iocross-/commit/fc4browser/cross-80b4f305e1device bi-directional6fe5972cf33device bi-directional6fe5972cf33for Socket.IO. An72dc44,uncaught exceptionhttps://githuvulnerability wasb.com/sockeintroduced intio/engine.ioversion 5.1.0 and/security/adincluded in versionvisories/GHS4.1.0 of theA-q9mw-	Vondor: sou	zkot		1090		
Affected Version(s): From (including) 5.1.0 Up to (excluding) 6.4.2Affected Version(s): From (including) 5.0 Up to (excluding) 6.4.2Engine.IO is the implementation of transport-based cross- browser/cross- device bi-directional device bi-directional for Socket.IO. An nucaught exception https://githu 						
N/A08-May-20236.5Engine.IO is the implementation of transport-based cross- device bi-directional for Socket.IO. An uncaught exception introduced in vulnerability was introduced in tio/engine.io for Socket.IO. and vulnerability was introduced in tio/engine.io for Socket.IO. and https://githu b.com/socke for Socket.IO. An vulnerability was introduced in tio/engine.io for Socket.IO. and tio/engine.io for Socket.IO. and https://githu b.com/socke introduced in tio/engine.ioA-SOC-ENGI- 170523/770N/A08-May-20236.56.5A-SOC-ENGI- 170523/770			cluding) 5	1.0 Up to (excluding) 6	4.2	
`socket.io` parent 68c2-j6m5				Engine.IO is the implementation of transport-based cross- browser/cross- device bi-directional communication layer for Socket.IO. An uncaught exception vulnerability was introduced in version 5.1.0 and included in version 4.1.0 of the	https://githu b.com/socke tio/engine.io /commit/fc4 80b4f305e1 6fe5972cf33 7d055e5983 72dc44, https://githu b.com/socke tio/engine.io /security/ad visories/GHS	

Page 407 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			package. Older versions are not impacted. A specially crafted HTTP request can trigger an uncaught exception on the Engine.IO server, thus killing the Node.js process. This impacts all the users of the `engine.io` package, including those who use depending packages like `socket.io`. This issue was fixed in version 6.4.2 of Engine.IO. There is no known workaround except upgrading to a safe version.					
CVE ID : CVE-2023- 31125								
_	onsors_carousel							
-	onsors_carouse							
Affected Ver	sion(s): * Up to (i	ncluding)	4.02					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Sergey Panasenko Sponsors Carousel plugin <= 4.02 versions. CVE ID : CVE-2023- 23808	N/A	A-SPO-SPON- 170523/771			
Vendor: sticky_ad_bar_project								
Product: sticky_ad_bar								
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10           Page 408 of 1106								

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): * Up to (i	including)	1.3.1	L	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Bon Plan Gratos Sticky Ad Bar plugin <= 1.3.1 versions. CVE ID : CVE-2023- 25784	N/A	A-STI-STIC- 170523/772
Vendor: str	ikingly				
Product: str					
Affected Ver					
Improperly Controlled Modificatio n of Object Prototype Attributes ('Prototype Pollution')	08-May-2023	6.1	A prototype pollution vulnerability exists in Strikingly CMS which can result in reflected cross-site scripting (XSS) in affected applications and sites built with Strikingly. The vulnerability exists because of Strikingly JavaScript library parsing the URL fragment allows access to the proto or constructor properties and the Object prototype. By leveraging an embedded gadget like jQuery, an attacker who convinces a victim to visit a specially crafted link could achieve arbitrary javascript execution	N/A	A-STR-STRI- 170523/773

0-1

1-2

**2-3** 3-4 4-5 Page **409** of **1106**  7-8

6-7

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the context of the user's browser.		
			CVE ID : CVE-2023- 2582		
Vendor: str	uktur		-	•	
Product: lib	heif				
Affected Ver	sion(s): 1.15.1			1	1
Divide By Zero	05-May-2023	6.5	A Segmentation fault caused by a floating point exception exists in libheif 1.15.1 using crafted heif images via the heif::Fraction::round () function in box.cc, which causes a denial of service. <b>CVE ID : CVE-2023- 29659</b>	N/A	A-STR-LIBH- 170523/774
Vendor: sup	oportcandy				
Product: su	pportcandy				
Affected Ver	sion(s): * Up to (e	excluding)	3.1.5		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	9.8	The SupportCandy WordPress plugin before 3.1.5 does not validate and escape user input before using it in an SQL statement, which could allow unauthenticated attackers to perform SQL injection attacks <b>CVE ID : CVE-2023-</b> <b>1730</b>	N/A	A-SUP-SUPP- 170523/775
Vendor: sur					
	pr_proof_cookie				
Affected Ver	sion(s): * Up to (e	excluding)	17.6.0		

0-1

1-2

2-33-44-5Page 410 of 1106

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	08-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Surbma Surbma   GDPR Proof Cookie Consent & Notice Bar plugin <= 17.5.3 versions.	N/A	A-SUR-GDPR- 170523/776	
Scripting')			CVE ID : CVE-2023- 23894			
Vendor: Sus	se					
Product: rai						
Affected Ver	sion(s): From (in	cluding) 2	.6.0 Up to (including) 2.	7.2		
	04-May-2023			Improper Privilege Management vulnerability in SUSE Rancher allows Privilege Escalation. A failure in the update logic of Rancher's admission Webhook may lead to		
Improper Privilege		23 9.9	the misconfiguration of the Webhook. This component enforces validation	https://bugz illa.suse.com /show_bug.c	A-SUS-RANC- 170523/777	
Manageme nt			rules and security checks before resources are admitted into the	gi?id=CVE- 2023-22651		
			Kubernetes cluster.			
			The issue only affects users that upgrade from 2.6.x or 2.7.x to 2.7.2. Users that did a fresh install of 2.7.2 (and did not follow an upgrade path) are not affected.			

0-1

1-2

2-33-44-5Page 411 of 1106

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22651		
Vendor: tap	filiate				
Product: tap	ofiliate				
Affected Vers	sion(s): * Up to (i	ncluding)	3.0.12		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Tapfiliate plugin <= 3.0.12 versions. CVE ID : CVE-2023- 25789	N/A	A-TAP-TAPF- 170523/778
Vendor: te-s	st			·	
Product: ya	ndex.news_feed	_by_tepli	tsa		
Affected Vers	sion(s): * Up to (e	excluding)	1.12.5		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site	08-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Teplitsa Yandex.News Feed by Teplitsa plugin <= 1.12.5 versions.	N/A	A-TEYAND- 170523/779
Scripting')			CVE ID : CVE-2023- 25052		
Vendor: Tea	impass		·		
Product: tea	impass				
Affected Vers	sion(s): * Up to (e	excluding)	3.0.7		
Improper Neutralizat ion of Input During Web Page Generation	05-May-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository nilsteampassnet/tea mpass prior to 3.0.7.	https://githu b.com/nilste ampassnet/t eampass/co mmit/39b77 4cba118ca5 383b0a51a7	A-TEA-TEAM- 170523/780
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3 3-4 4-5 5-6</b> Page <b>412</b> of <b>1106</b>	5 <u>6-7</u> 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			CVE ID : CVE-2023- 2516	1b1e7dea27 61927, https://hunt r.dev/bounti es/19470f0b -7094-4339- 8d4a- 4b5570b547 16	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in GitHub repository nilsteampassnet/tea mpass prior to 3.0.7. <b>CVE ID : CVE-2023- 2591</b>	https://hunt r.dev/bounti es/705f79f4- f5e3-41d7- 82a5- f00441cd98 4b, https://githu b.com/nilste ampassnet/t eampass/co mmit/57a97 7c6323656e 5dc06ab5c2 27e75c3465 a1a4a	A-TEA-TEAM- 170523/781
Vendor: the	meisle				
Product: vis	sualizer				
Affected Ver	sion(s): * Up to (e	excluding)	3.9.5		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Themeisle Visualizer: Tables and Charts Manager for WordPress plugin <= 3.9.4 versions. <b>CVE ID : CVE-2023-</b>	N/A	A-THE-VISU- 170523/782
17			23708		
Vendor: tim	ersys				

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wj	p_popups	1			1
Affected Ver	sion(s): * Up to (	excluding)	2.1.5.1		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	The WP Popups WordPress plugin before 2.1.5.1 does not properly escape the href attribute of its spu-facebook- page shortcode before outputting it 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. This is due to an insufficient fix of CVE-2023-24003 <b>CVE ID : CVE-2023-</b> <b>1905</b>	N/A	A-TIM-WP_P- 170523/783
	osandtricks-hq				
Product: ca	tegory_specific_	rss_feed_s	subscription		
Affected Ver	sion(s): * Up to (	excluding)	2.2		
Cross-Site Request Forgery (CSRF)	03-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Tips and Tricks HQ, Ruhul Amin Category Specific RSS feed Subscription plugin <= v2.1 versions. <b>CVE ID : CVE-2023- 22691</b>	N/A	A-TIP-CATE- 170523/784
Vendor: tm	s-outsource			<u> </u>	l
Product: wj	odatatables				
Affected Ver	sion(s): * Up to (	excluding)	2.1.50		

Page **414** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site	03-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in TMS- Plugins wpDataTables plugin <= 2.1.49 versions. <b>CVE ID : CVE-2023-</b>	N/A	A-TMS-WPDA- 170523/785
Scripting')	digitaltuan da		23876		
	digitaltrends ga_addons_for_	umbalian	u naga huildan		
	sion(s): * Up to (e	-			
			The Mega Addons		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	For WPBakery Page Builder WordPress plugin before 4.3.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023- 0268</b>	N/A	A-TOP-MEGA- 170523/786
	imate_carousel				
Affected Vers	sion(s): * Up to (i	ncluding)			
Improper Neutralizat ion of Input During Web Page Generation	08-May-2023	5.4	The Ultimate Carousel For Elementor WordPress plugin through 2.1.7 does not validate and escape some of its block options before	N/A	A-TOP-ULTI- 170523/787
CVSS Scoring S	cale 0-1 2	1-2 2-3	3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Page **415** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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. <b>CVE ID : CVE-2023-</b> <b>0280</b>		
Product: ult	imate carousel	for wpba	akery_page_builder		
	sion(s): * Up to (i	_			
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	The Ultimate Carousel For WPBakery Page Builder WordPress plugin through 2.6 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. <b>CVE ID : CVE-2023- 0267</b>	N/A	A-TOP-ULTI- 170523/788
Vendor: tor					
Affected Ver	sm sion(s): 1.3.0				
Missing Release of Memory after	09-May-2023	9.8	yasm v1.3.0 was discovered to contain a memory leak via the function yasm_intnum_copy	N/A	A-TOR-YASM- 170523/789
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>416</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		at /libyasm/intnum.c. CVE ID : CVE-2023- 31975		
09-May-2023	7.8	yasm v1.3.0 was discovered to contain a use after free via the function pp_getline at /nasm/nasm-pp.c. <b>CVE ID : CVE-2023-</b> <b>31972</b>	N/A	A-TOR-YASM- 170523/790
09-May-2023	7.8	yasm v1.3.0 was discovered to contain a use after free via the function expand_mmac_para ms at /nasm/nasm- pp.c. <b>CVE ID : CVE-2023-</b> <b>31973</b>	N/A	A-TOR-YASM- 170523/791
09-May-2023	7.8	yasm v1.3.0 was discovered to contain a use after free via the function error at /nasm/nasm-pp.c. <b>CVE ID : CVE-2023-</b> <b>31974</b>	N/A	A-TOR-YASM- 170523/792
al-soft			·	·
deo_gallery	1 1	1.0.0		
sion(s): * Up to (e	excluding)			
03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Video Gallery by Total-Soft Video Gallery plugin <= 1.7.6 versions.	N/A	A-TOT-VIDE- 170523/793
(	09-May-2023 09-May-2023 09-May-2023 09-May-2023	09-Мау-2023         7.8           09-Мау-2023         7.8           09-Мау-2023         7.8           09-Мау-2023         7.8           09-Мау-2023         7.8           09-Мау-2023         7.8           09-Мау-2023         7.8	at /libyasm/intnum.c.09-May-20237.8at /libyasm/intnum.c.09-May-20237.8yasm v1.3.0 was discovered to contain a use after free via the function pp_getline at /nasm/nasm-pp.c.09-May-20237.8yasm v1.3.0 was discovered to contain a use after free via the function expand_mmac_para ms at /nasm/nasm-pp.c.09-May-20237.8yasm v1.3.0 was discovered to contain a use after free via the function expand_mmac_para ms at /nasm/nasm-pp.c.09-May-20237.8yasm v1.3.0 was discovered to contain a use after free via the function expand_mmac_para ms at /nasm/nasm-pp.c.09-May-20237.8yasm v1.3.0 was discovered to contain a use after free via the function error at /nasm/nasm-pp.c.09-May-20237.8Yasm v1.3.0 was discovered to contain a use after free via the function error at /nasm/nasm-pp.c.09-May-20234.8Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Video Gallery by Total-Soft Video	at /libyasm/intnum.c. CVE ID : CVE-2023- 31975at /libyasm/intnum.c. CVE ID : CVE-2023- 3197509-May-20237.8yasm v1.3.0 was 

Page 417 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
('Cross-site Scripting')			CVE ID : CVE-2023- 25979							
Vendor: tota	aljs									
Product: flo	w									
Affected Ver	Affected Version(s): 10.0									
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in TotalJS Flow v10 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the platform name field in the settings module. <b>CVE ID : CVE-2023-</b>	https://githu b.com/totalj s/flow/issue s/100	A-TOT-FLOW- 170523/794					
			CVE ID : CVE-2023- 30094							
Product: me										
Affected Ver	sion(s): -									
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in TotalJS messenger commit b6cf1c9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the channel description field. <b>CVE ID : CVE-2023-</b>	https://githu b.com/totalj s/messenger /issues/11	A-TOT-MESS- 170523/795					
			30095							
Improper Neutralizat ion of Input During Web Page	04-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in TotalJS messenger commit b6cf1c9 allows attackers to	https://githu b.com/totalj s/messenger /issues/10	A-TOT-MESS- 170523/796					

0-1

1-2

**2-3** 3-4 4-5 Page **418** of **1106**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			execute arbitrary web scripts or HTML via a crafted payload injected into the user information field.		
			CVE ID : CVE-2023- 30096		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in TotalJS messenger commit b6cf1c9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the private task field. <b>CVE ID : CVE-2023-</b> <b>30097</b>	https://githu b.com/totalj s/messenger /issues/9	A-TOT-MESS- 170523/797
Vendor: trib	pe29		50077		
Product: ch	eckmk				
Affected Ver	sion(s): 2.0.0				
Insertion of Sensitive Informatio n into Log File	02-May-2023	5.5	Transmission of credentials within query parameters in Checkmk <= 2.1.0p26, <= 2.0.0p35, and <= 2.2.0b6 (beta) may cause the automation user's secret to be written to the site Apache access log. <b>CVE ID : CVE-2023-</b>	https://chec kmk.com/we rk/15189	A-TRI-CHEC- 170523/798
			31207		
Affected Ver	sion(s): 2.1.0				

0-1

1-2

**2-3** 3-4 4-5 Page **419** of **1106**  5-6

6-7 7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Informatio n into Log File	02-May-2023	5.5	Transmission of credentials within query parameters in Checkmk <= 2.1.0p26, <= 2.0.0p35, and <= 2.2.0b6 (beta) may cause the automation user's secret to be written to the site Apache access log. <b>CVE ID : CVE-2023-</b>	https://chec kmk.com/we rk/15189	A-TRI-CHEC- 170523/799
Affected Ver	sion(s), 220		31207		
Allected ver	sion(s): 2.2.0		m i i c		
Insertion of Sensitive Informatio n into Log File	02-May-2023	5.5	Transmission of credentials within query parameters in Checkmk <= 2.1.0p26, <= 2.0.0p35, and <= 2.2.0b6 (beta) may cause the automation user's secret to be written to the site Apache access log. <b>CVE ID : CVE-2023-</b> <b>31207</b>	https://chec kmk.com/we rk/15189	A-TRI-CHEC- 170523/800
Vendor: trit	on_project				I
Product: tri	ton				
Affected Ver	sion(s): * Up to (e	excluding)	3.7.5		
N/A	01-May-2023	9.8	Triton is a Minecraft plugin for Spigot and BungeeCord that helps you translate your Minecraft server. The CustomPayload packet allows you to execute commands	https://githu b.com/triton mc/Triton/s ecurity/advi sories/GHSA -8vj5-jccf- q25r	A-TRI-TRIT- 170523/801

0-1

1-2

**2-3** 3-4 4-5 Page **420** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the spigot/bukkit		
			console. When you		
			enable bungee mode		
			in the config it will		
			enable the bungee		
			bridge and the		
			server will begin to broadcast the		
			'triton:main' plugin		
			channel. Using this		
			plugin channel you		
			are able to send a		
			payload packet		
			containing a byte (2)		
			and a string (any		
			spigot command).		
			This could be used to		
			make yourself a		
			server operator and		
			be used to extract		
			other user		
			information through		
			phishing (pretending		
			to be an admin),		
			many servers use		
			essentials so the		
			/geoip command		
			could be available to		
			them, etc. This could		
			also be modified to		
			allow you to set the		
			servers language, set		
			another players		
			language, etc. This issue affects those		
			who have bungee		
			enabled in config.		
			This issue has been		
			fixed in version 3.8.4.		
			CVE ID : CVE-2023-		
			30859		
				0.4	
Affected Vers	sion(s): From (in	cluding) 3	.8.0 Up to (excluding) 3	.ö.4	

0-1

1-2

2-33-44-5Page 421 of 1106

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	9.8	Triton is a Minecraft plugin for Spigot and BungeeCord that helps you translate your Minecraft server. The CustomPayload packet allows you to execute commands on the spigot/bukkit console. When you enable bungee mode in the config it will enable the bungee bridge and the server will begin to broadcast the 'triton:main' plugin channel. Using this plugin channel you are able to send a payload packet containing a byte (2) and a string (any spigot command). This could be used to make yourself a server operator and be used to extract other user information through phishing (pretending to be an admin), many servers use essentials so the /geoip command could be available to them, etc. This could also be modified to allow you to set the servers language, set another players language, etc. This issue affects those	https://githu b.com/triton mc/Triton/s ecurity/advi sories/GHSA -8vj5-jccf- q25r	A-TRI-TRIT- 170523/802

0-1

1-2

2-33-44-5Page 422 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			who have bungee enabled in config. This issue has been fixed in version 3.8.4.		
			CVE ID : CVE-2023- 30859		
Vendor: typ	echo				
Product: typ	pecho				
Affected Ver	sion(s): * Up to (i	ncluding)	1.2.0		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in Typecho v1.2.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the url parameter at /index.php/archives /1/comment. <b>CVE ID : CVE-2023-</b>	N/A	A-TYP-TYPE- 170523/803
x7 1 1			30184		
	omemorydirect	<u>+  </u>	<u>Glas</u>		
	nple_custom_au				
Allected ver	<mark>sion(s): * Up to (</mark> i	including			1
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site	09-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in USB Memory Direct Simple Custom Author Profiles plugin <= 1.0.0 versions.	N/A	A-USB-SIMP- 170523/804
Scripting')			CVE ID : CVE-2023- 24372		
Vendor: use	erlike				· · · · · · · · · · · · · · · · · · ·
Product: us	erlike				

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): * Up to (e	excluding)	2.3		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in David Voswinkel Userlike – WordPress Live Chat plugin <= 2.2 versions. CVE ID : CVE-2023- 23734	N/A	A-USE-USER- 170523/805
Vendor: ver	tical_scroll_rece	ent_post_j	project		
Product: ve	rtical_scroll_rec	ent_post			
Affected Ver	sion(s): * Up to (i	including)	14.0		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Vertical scroll recent post plugin <= 14.0 versions. <b>CVE ID : CVE-2023-</b> <b>23862</b>	N/A	A-VER-VERT- 170523/806
Vendor: VIN	1			1	
Product: vir	n				
Affected Ver	sion(s): * Up to (e	excluding)	9.0.1532		
Integer Overflow or Wraparoun d	09-May-2023	7.8	Integer Overflow or Wraparound in GitHub repository vim/vim prior to 9.0.1532. <b>CVE ID : CVE-2023-</b> <b>2610</b>	https://githu b.com/vim/v im/commit/ ab9a2d884b 3a4abe3196 06ea95a5a6 d6b01cd73a, https://hunt r.dev/bounti es/31e6734 0-935b-4f6c- a923-	A-VIM-VIM- 170523/807

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				f7246bc29c7 d	
Vondor: vir	tualreception			u	
	•				
	gital_reciptie	utra 1011		7702	
Allected ver	sion(s): win/spi	_rum.1011	.19-1850_6.1.7601.1.0.6	5/92	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-May-2023	7.5	Directory Traversal vulnerability in virtualreception Digital Receptie version win7sp1_rtm.10111 9-1850 6.1.7601.1.0.65792 in embedded web server, allows attacker to gain sensitive information via a crafted GET request. <b>CVE ID : CVE-2023- 25289</b>	N/A	A-VIR-DIGI- 170523/808
Vendor: vk.	company				1
Product: my	ymail				
Affected Ver	sion(s): * Up to (i	ncluding)	14.30		
Missing Encryption of Sensitive Data	07-May-2023	7.5	The myMail app through 14.30 for iOS sends cleartext credentials in a situation where STARTTLS is expected by a server. <b>CVE ID : CVE-2023-</b> <b>32290</b>	https://mail box.org/en/ post/mailbo x-org- discovers- unencrypted -password- transmission -in-mymail	A-VKMYMA- 170523/809
Vendor: vsli	ider_multi_imag	e_slider_j	project		
Product: vs	lider_multi_ima	ge_slider			
Affected Ver	sion(s): * Up to (i	ncluding)	4.1.2		
Improper Neutralizat ion of	03-May-2023	4.8	Auth. Stored Cross- Site Scripting (XSS) vulnerability in	N/A	A-VSL-VSLI- 170523/810

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

 Page 425 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Input During Web Page Generation ('Cross-site Scripting')			Mr.Vibe vSlider Multi Image Slider for WordPress plugin <= 4.1.2 versions. CVE ID : CVE-2023- 25797					
Vendor: W3								
Product: we	bassembly							
Affected Vers	sion(s): 1.0							
Loop with Unreachabl e Exit Condition ('Infinite Loop')	03-May-2023	5.5	An issue in the component hang.wasm of WebAssembly 1.0 causes an infinite loop. <b>CVE ID : CVE-2023-</b> <b>30300</b>	N/A	A-W3-WEBA- 170523/811			
Vendor: web_design_easy_sign_up_project								
Product: we	b_design_easy_s	sign_up						
Affected Vers	sion(s): * Up to (i	ncluding)	3.4.1					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	10-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Andrew @ Geeenville Web Design Easy Sign Up plugin <= 3.4.1 versions. CVE ID : CVE-2023- 23701	N/A	A-WEB-WEB 170523/812			
Vendor: win	iterchen							
Product: my	/-site							
Affected Vers	sion(s): * Up to (e	excluding)	2023-03-30					
Improper Neutralizat ion of Input During	01-May-2023	5.4	Cross Site Scripting (XSS) vulnerability in WinterChenS my-site before commit 3f0423da6d5200c7a	https://githu b.com/Winte rChenS/my-	A-WIN-MY-S- 170523/813			
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b>	6-7 7-8	8 8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			46e200da145c1f54e e18548, allows attackers to inject arbitrary web script or HTML via editing blog articles. <b>CVE ID : CVE-2023-</b>	site/issues/7 4	
			29638		
Vendor: wir	iwar				
-	o_email_capture				
Affected Ver	sion(s): * Up to (e	excluding)		1	
Improper Neutralizat ion of Input During Web Page Generation	02-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Winwar Media WP Email Capture plugin <= 3.9.3 versions.	N/A	A-WIN-WP_E- 170523/814
('Cross-site Scripting')			CVE ID : CVE-2023- 23723		
Vendor: wjj	soft				
Product: ini	ıokb				
Affected Ver	sion(s): 2.2.1				-
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-May-2023	7.5	WJJ Software - InnoKB Server, InnoKB/Console 2.2.1 - CWE-22: Path Traversal CVE ID : CVE-2023- 31181	N/A	A-WJJ-INNO- 170523/815
Improper Neutralizat ion of Input During	08-May-2023	6.1	WJJ Software - InnoKB Server, InnoKB/Console	N/A	A-WJJ-INNO- 170523/816

Page 427 of 1106

Web Page Generation ('Cross-site Scripting')			2.2.1 - Reflected cross-site scripting (RXSS) through an unspecified request.		
			CVE ID : CVE-2023- 31180		
Vendor: wpdov	_	-			
Product: down			0 0 Up to (oveluding) 6	2.0	
Allected versio		Juung 6	.0.0 Up to (excluding) 6	.3.0	
N/A 02	2-May-2023	7.5	The Download Manager WordPress plugin before 6.3.0 leaks master key information without the need for a password, allowing attackers to download arbitrary password-protected package files. <b>CVE ID : CVE-2023-</b> <b>1809</b>	N/A	A-WPD-DOWN- 170523/817
Product: guter	nberg_blocks_t	for_word	press_download_man	ager	
Affected Version	on(s): * Up to (e	xcluding)	2.1.9		
Improper Neutralizat ion of Input During 03 Web Page Generation ('Cross-site Scripting')	'3-May-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress Download Manager Gutenberg Blocks by WordPress Download Manager plugin <= 2.1.8 versions. <b>CVE ID : CVE-2023-</b> <b>22713</b>	N/A	A-WPD-GUTE- 170523/818
Vendor: wpinv	ventory				

0-1

1-2

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wp	_inventory_mai	nager		L	
Affected Ver	sion(s): * Up to (e	excluding)	2.1.0.12		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	6.1	The WP Inventory Manager WordPress plugin before 2.1.0.12 does not sanitise and escape the message 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 administrators. <b>CVE ID : CVE-2023-</b>	N/A	A-WPI-WP_I- 170523/819
			1806		
Vendor: wp					
	am_memberte				
Affected Ver	sion(s): * Up to (i	ncluding)	4.4	1	
Improper Neutralizat ion of Input During Web Page Generation	09-May-2023	5.4	Auth. (author+) Stored Cross-Site Scripting (XSS) vulnerability in Sk. Abul Hasan Team Member – Team with Slider plugin <= 4.4 versions.	N/A	A-WPM-TEAM- 170523/820
('Cross-site Scripting')			CVE ID : CVE-2023- 23647		
Vendor: wp	mobile.app_pro	ject			
Product: wp	omobile.app				
Affected Ver	sion(s): * Up to (e	excluding)	11.19		
Improper Neutralizat ion of Input During	04-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPMobile.App	N/A	A-WPM-WPMO- 170523/821
0	1		1 F	1	-1
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4 4-5 5-6	6-7 7	-8 8-9 9-10

<mark>9_desk</mark> * Up to (	excluding)	The Ruby Help Desk		
	excluding)	The Ruby Help Desk		
	excluding)	The Ruby Help Desk		
* Up to (	excluding)	The Ruby Help Desk		
		· ·		
y-2023	6.5	WordPress plugin before 1.3.4 does not ensure that the ticket being modified belongs to the user making the request, allowing an attacker to close and/or add files and replies to tickets other than their own.	N/A	A-WPR-RUBY- 170523/822
		CVE ID : CVE-2023- 1125		
_submit_j	project			
_submit				
* Up to (	including)			1
y-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Include WP BaiDu Submit plugin <= 1.2.1 versions. CVE ID : CVE-2023- 25796	N/A	A-WPWP_B- 170523/823
nt_filter_·	censor_a	all_offensive_content_f	rom_your_site	_project
nt_filter_	censor_	all_offensive_content_	from_your_site	e
¥ 11	including)	3.0.1		
* Up to (1	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS)	N/A	A-WPWP_C- 170523/824
		* Up to (including)	* Up to (including) 3.0.1y-2023Auth. (admin+) Stored Cross-Site	y-2023 4.8 Auth. (admin+) Stored Cross-Site N/A Scripting (XSS)

Page 430 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			vulnerability in David Gwyer WP Content Filter plugin <= 3.0.1 versions. CVE ID : CVE-2023- 23883		
Vendor: wp	_custom_author	_url_proj	ect		
Product: wp	o_custom_autho	r_url			
Affected Ver	sion(s): * Up to (e	excluding)	1.0.5		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	4.8	The WP Custom Author URL WordPress plugin before 1.0.5 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). <b>CVE ID : CVE-2023-</b> <b>1614</b>	N/A	A-WPWP_C- 170523/825
Vendor: wp	_login_box_proj	ect			
Product: wp	- 01 /				
Affected Ver	sion(s): * Up to (i	ncluding)	2.0.2		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	4.8	The WP Login Box WordPress plugin through 2.0.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting	N/A	A-WPWP_L- 170523/826
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 - 2 - 3	Page <b>431</b> of <b>1106</b>	, , , , , , , , , , , , , , , , , , , ,	0 0-9 0-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)		
			CVE ID : CVE-2023- 0544		
Vendor: wp	_open_social_pr	oject		I	
Product: wp	o_open_social				
Affected Ver	sion(s): * Up to (i	ncluding)	5.0		
Improper Neutralizat ion of Input During Web Page Generation	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in XiaoMac WP Open Social plugin <= 5.0 versions.	N/A	A-WPWP_0- 170523/827
('Cross-site Scripting')			CVE ID : CVE-2023- 25792		
Vendor: wp	_resource_down	load_ma	nagement_project	1	
Product: wp	o_resource_dow	nload_ma	nagement		
Affected Ver	sion(s): * Up to (i	ncluding)	1.3.9		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Wbolt team WP????? plugin <= 1.3.9 versions. CVE ID : CVE-2023- 25787	N/A	A-WPWP_R- 170523/828
Vendor: wp	_simple_events_	project			
Product: wp	o_simple_events				
Affected Ver	sion(s): * Up to (i	ncluding)	1.0		
Improper Neutralizat ion of Input	08-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Nico	N/A	A-WPWP_S- 170523/829
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4 4-5 5-6	6-7 7-	8 8-9 9-10
UV2220000085		L-Z Z-3		, 0-/ /-	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation			Graff WP Simple Events plugin <= 1.0 versions.		
('Cross-site Scripting')			CVE ID : CVE-2023- 24376		
Vendor: Zar	nmad			<u> </u>	
Product: Za	mmad				
Affected Ver	sion(s): From (in	cluding) 5	.3.0 Up to (excluding) 5	.4.0	
N/A	02-May-2023	6.5	Zammad 5.3.x (Fixed 5.4.0) is vulnerable to Incorrect Access Control. An authenticated attacker could gain information about linked accounts of users involved in their tickets using the Zammad API.	https://zam mad.com/en /advisories/ zaa-2023-02	A-ZAM-ZAMM- 170523/830
			CVE ID : CVE-2023- 29867		
N/A	02-May-2023	6.5	Zammad 5.3.x (Fixed in 5.4.0) is vulnerable to Incorrect Access Control. An authenticated attacker with agent and customer roles could perform unauthorized changes on articles where they only have customer permissions. <b>CVE ID : CVE-2023-</b>	https://zam mad.com/en /advisories/ zaa-2023-01	A-ZAM-ZAMM- 170523/831
Vander			29868		
	enfeng13_my-blo		t		
	enfeng13_my-bl	og			
Affected Ver	sion(s): -				

0-1

1-2

2-33-44-5Page 433 of 1106

5-6

6-7

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')0.1-May-20235.4Cross site scripting (XSS) vulnerability in ZHENFENGASIMY- Blog, allows attackers to inject arbitrary web script or HTML via the "title" field in the "blog management" page due to the the default configuration not using MyBlogUtils.cleanStri ing.https://githu brom/ZHEN A-ZHE-ZHEN- TO523/832Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')0.1-May-2023S.4Cross site scripting (XSS) vulnerability in ZHENFENGAS My- Blog, allows attackers to inject arbitrary web script or HTML via editing an arbitrary web script or HTML via editing arbitrary web script or HTML via editing matricle in the "blog management" blog.allows attackers to inject arbitrary web script or HTML via editing matricle in the "blog for HTML via editing matricle in the "blog management" page due to the default configuration not utilizing MyBlogUtils.cleanStri ing. CVE ID : CVE-2023- 29639A-ZHE-ZHEN- A-ZHE-ZHEN- 170523/833Vendor: Zo-verFFV-Product: maageengine_opmanager Scripting')0.4-May-20238.8Zoho ManageEngine COPManager through 126323 allows an athenticated user to codehttps://ww wmanageeng monitoring/ achiever wet codehttps://ww wmanageeng monitoring/ achiever end codeA-ZOH-MANA- 170523/834N/A0.4-May-20238.8Zoho ManageEngine achiever end codehttps://ww wmanageeng monitoring/ achiever end codehttps://ww wmanageeng monitoring/	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')1(XSS) vulnerability in ZHENFENG13 My- Blog, allows attackers to inject arbitrary web script or HTML via editing an article in the "blog article" page due to the default configuration not utilizing MyBlogUtis.cleanStri ing. CVE ID : CVE-2023- 29639https://githu b.com/ZHEN Blog/issues/ 131A-ZHE-ZHEN- A-ZHE-ZHEN- 170523/833Vendor: Z-VerorZoho Manage Ingine OPManager through 126323 allows an authenticated user to achieve remote codehttps://ww wwmanagen gine.com/ne work- monitoring/ security- updates/cveA-ZHE-ZHEN- A-ZHE-ZHE-ZHE- A-ZHE-ZHE-ZHE- A-ZHE-ZHE-ZHE- A-ZHE-ZHE-ZHE-ZHE- A-ZHE-ZHE-ZHE-ZHE-ZHE-ZHE-ZHE-ZHE-ZHE-ZHE	Neutralizat ion of Input During Web Page Generation ('Cross-site	01-May-2023	5.4	(XSS) vulnerability in ZHENFENG13 My- Blog, allows attackers to inject arbitrary web script or HTML via the "title" field in the "blog management" page due to the the default configuration not using MyBlogUtils.cleanStr ing. <b>CVE ID : CVE-2023-</b>	b.com/ZHEN FENG13/My- Blog/issues/	
Product: marage=rgine_op=rate       Image: Signe op in the signe op in	Neutralizat ion of Input During Web Page Generation ('Cross-site	01-May-2023	5.4	(XSS) vulnerability in ZHENFENG13 My- Blog, allows attackers to inject arbitrary web script or HTML via editing an article in the "blog article" page due to the default configuration not utilizing MyBlogUtils.cleanStr ing. <b>CVE ID : CVE-2023-</b>	b.com/ZHEN FENG13/My- Blog/issues/	
Affected Version(s): * Up to (excluding) 12.6         N/A       04-May-2023       8.8       Zoho ManageEngine OPManager through 126323 allows an authenticated user to achieve remote code       https://ww w.manageen gine.com/ne twork- monitoring/ achieve remote code       A-ZOH-MANA- 170523/834         V/SS Scoring Scale       0-1       1-2       2-3       3-4       4-5       5-6       6-7       7-8       8-9       9-10	Vendor: Zol	ıocorp				
N/A       04-May-2023       8.8       Zoho ManageEngine OPManager through 126323 allows an authenticated user to achieve remote code       https://ww       A-ZOH-MANA-170523/834         V/A       04-May-2023       8.8       Zoho ManageEngine OPManager through 126323 allows an authenticated user to achieve remote code       https://ww       A-ZOH-MANA-170523/834         V/A       04-May-2023       8.8       3-4       4-5       5-6       6-7       7-8       8-9       9-10	Product: ma	anageengine_op	manager			
N/A       04-May-2023       8.8       Zoho ManageEngine OPManager through 126323 allows an authenticated user to achieve remote code       w.manageen gine.com/ne twork- monitoring/ security- updates/cve-       A-ZOH-MANA- 170523/834         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 (	excluding)	12.6		
	N/A	04-May-2023	8.8	OPManager through 126323 allows an authenticated user to	w.manageen gine.com/ne twork- monitoring/ security-	-
	CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>434</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution via probe servers.	2023- 31099.html	
			CVE ID : CVE-2023- 31099		
Affected Ver	sion(s): 12.6				
N/A	04-May-2023	8.8	Zoho ManageEngine OPManager through 126323 allows an authenticated user to achieve remote code execution via probe servers. <b>CVE ID : CVE-2023-</b> <b>31099</b>	https://ww w.manageen gine.com/ne twork- monitoring/ security- updates/cve- 2023- 31099.html	A-ZOH-MANA- 170523/835
Vendor: zyr	ex				
Product: po					
Affected Ver	sion(s): * Up to (e	excluding)	1.1		
Unrestricte d Upload of File with Dangerous Type	02-May-2023	7.2	The ZYREX POPUP WordPress plugin through 1.0 does not validate the type of files uploaded when creating a popup, allowing a high privileged user (such as an Administrator) to upload arbitrary files, even when modifying the file system is disallowed, such as in a multisite install. <b>CVE ID : CVE-2023- 0924</b>	N/A	A-ZYR-POPU- 170523/836
			Hardware		
Vendor: Adv					
Product: ek					
Affected Ver	sion(s): -				

0-1

1-2

2-33-44-5Page 435 of 1106

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the NTP server input field, which can be triggered by authenticated users via a crafted POST request. CVE ID : CVE-2023- 2573	https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBL	H-ADV-EKI 170523/837
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the device name input field, which can be triggered by authenticated users via a crafted POST request. <b>CVE ID : CVE-2023- 2574</b>	https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBL	H-ADV-EKI 170523/838
Out-of- bounds Write	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stack-based Buffer Overflow	https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3,	H-ADV-EKI 170523/839

0-1

1-2

**2-3** 3-4 4-5 Page **436** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, which can be triggered by authenticated users via a crafted POST request. <b>CVE ID : CVE-2023-</b> <b>2575</b>	https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBL	
Product: ek					
Affected Ver	sion(s): -		Advantech EKI-1524,		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the NTP server input field, which can be triggered by authenticated users via a crafted POST request. CVE ID : CVE-2023- 2573	https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBL	H-ADV-EKI 170523/840
Improper Neutralizat ion of Special Elements used in a Command ('Comman	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the device name input field, which can be triggered by	https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3, https://ww w.advantech. com/en/sup	H-ADV-EKI 170523/841

0-1

1-2

**2-3** 3-4 4-5 Page **437** of **1106** 

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
d Injection')			authenticated users via a crafted POST request. CVE ID : CVE-2023- 2574	port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBL			
Out-of- bounds Write	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stack-based Buffer Overflow vulnerability, which can be triggered by authenticated users via a crafted POST request. <b>CVE ID : CVE-2023- 2575</b>	https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBL	H-ADV-EKI 170523/842		
Product: eki	i-1524						
Affected Vers	sion(s): -						
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the NTP server input field, which can be triggered by authenticated users via a crafted POST request.	https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech.	H-ADV-EKI 170523/843		
w.advantech.							

Improper Neutralizat ion of Special Elements used in a Command ('Comman d08-May-20238.8Advantech EKI-1524, EKI-1522, EKI-1521 are affected by an command injection triggered by authenticated users via a crafted POST request.https://ww w.advante com/en/su port/detai firmware? e1-1J9BEDImproper Neutralizat ion of Special Elements used in a Command ('Comman08-May-20238.8Advantech EKI-1524, etriggered by authenticated users via a crafted POST request.https://ww w.advante	v ch. up ls/ d
Improper Neutralizat ion of Special Elements used in a Command ('Comman dAdvantech EKI-1524, EKI-1522, EKI-1521 are affected by an command injection firmware? 	ch. ip s/ d
Injection J       w.advante         CVE ID : CVE-2023-       com/en/su         2574       firmware?         =1-1J9BEE	v ch. ip H-ADV-EKI is/ 170523/844 d T, v ch. ip is/ d
Out-of- bounds08-May-20238.8Advantech EKI-1522, EKI-1521 devices through 1.21 are affected by a Stack-based Buffer Overflowhttps://www.advante com/en/su 9ort/detai firmware? =1-1J9BED https://www.advante com/en/su port/detai firmware? =1-1J9BED https://www.advante com/en/su port/detai firmware? =1-1J9BED https://www.advante com/en/su port/detai firmware? =1-1J9BED https://www.advante com/en/su port/detai firmware? =1-1J9BED https://www.advante com/en/su port/detai firmware? =1-1J9BED https://www.advante com/en/su port/detai firmware? =1-1J9BED 	ch. p s/ d 3, v ch. p H-ADV-EKI s/ 170523/845 d T, v ch. p s/ d 4 170523/845 d 170523/845 d 17057 17057
Vendor: aigital	
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7	7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Product: wi	reless-n_repeat	er_mini_r	outer	L				
Affected Ver	sion(s): -							
Insufficient Session Expiration	02-May-2023	7.5	An issue in the time- based authentication mechanism of Aigital Aigital Wireless-N Repeater Mini_Router v0.131229 allows attackers to bypass login by connecting to the web app after a successful attempt by a legitimate user.	N/A	H-AIG-WIRE- 170523/846			
			CVE ID : CVE-2023- 30403					
Vendor: Am	azon			<u> </u>				
Product: fire_tv_stick_3rd_gen								
Affected Ver	sion(s): -							
Use of Insufficient ly Random Values	03-May-2023	8.8	Improper JPAKE implementation allows offline PIN brute-forcing due to the initialization of random values to a known value, which leads to unauthorized authentication to amzn.lightning services. This issue affects: Amazon Fire TV Stick	N/A	H-AMA-FIRE- 170523/847			
			3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS 7.6.3.3.					

0-1

1-2

**2-3** 3-4 4-5 Page **440** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 1385		
Improper Neutralizat ion of			The setMediaSource function on the amzn.thin.pl service does not sanitize the "source" parameter allowing for arbitrary javascript code to be run		
Input During Web Page Generation ('Cross-site	03-May-2023	6.1	This issue affects: Amazon Fire TV Stick	N/A	H-AMA-FIRE- 170523/848
Scripting')			3rd gen versions prior to 6.2.9.5.		
			Insignia TV with FireOS versions prior to 7.6.3.3.		
			CVE ID : CVE-2023- 1384		
N/A	03-May-2023	4.3	An Improper Enforcement of Behavioral Workflow vulnerability in the exchangeDeviceServi ces function on the amzn.dmgr service allowed an attacker to register services that are only locally accessible.	N/A	H-AMA-FIRE- 170523/849
			This issue affects:		
			Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5.		

0-1

1-2

2-33-44-5Page 441 of 1106

5-6

6-7

7-8 8-9 9-10

	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Insignia TV with FireOS versions prior to 7.6.3.3.		
			CVE ID : CVE-2023- 1383		
Vendor: Ap	ple				
Product: stu	idio_display				
Affected Ver	sion(s): -		-	-	-
Out-of- bounds Write	08-May-2023	7.8	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, Studio Display Firmware Update 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023-</b>	https://supp ort.apple.co m/en- us/HT21367 2, https://supp ort.apple.co m/en- us/HT21367 0	H-APP-STUD- 170523/850
Vendor: Ası	15		27965		
Product: rt-					
Affected Ver	sion(s): -				
(mproper Neutralizat on of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	5.2	A Cross-site scripting (XSS) vulnerability in the System Log/General Log page of the administrator web UI in ASUS RT- AC51U wireless router firmware version up to and including 3.0.0.4.380.8591 allows remote attackers to inject arbitrary web script	N/A	H-ASU-RT-A- 170523/851
	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
			or HTML via a malicious network request.		
			CVE ID : CVE-2023- 29772		
Vendor: bes	stbuy				
Product: ins	signia_tv				
Affected Ver	sion(s): -				
Use of Insufficient ly Random Values	03-May-2023	8.8	Improper JPAKE implementation allows offline PIN brute-forcing due to the initialization of random values to a known value, which leads to unauthorized authentication to amzn.lightning services. This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS 7.6.3.3. <b>CVE ID : CVE-2023-</b> <b>1385</b>	N/A	H-BES-INSI- 170523/852
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	The setMediaSource function on the amzn.thin.pl service does not sanitize the "source" parameter allowing for arbitrary javascript code to be run	N/A	H-BES-INSI- 170523/853

0-1

1-2

5-6 6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects:		
			Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5.		
			Insignia TV with FireOS versions prior to 7.6.3.3.		
			CVE ID : CVE-2023- 1384		
			An Improper Enforcement of Behavioral Workflow vulnerability in the exchangeDeviceServi ces function on the amzn.dmgr service allowed an attacker to register services that are only locally accessible.		
N/A	03-May-2023	4.3	This issue affects:	N/A	H-BES-INSI- 170523/854
			Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5.		
			Insignia TV with FireOS versions prior to 7.6.3.3.		
			CVE ID : CVE-2023- 1383		
Vendor: Cis	со	I			
Product: sp	a112				
Affected Ver	sion(s): -				
Missing Authentica tion for	04-May-2023	9.8	A vulnerability in the web-based management interface of Cisco	https://sec.c loudapps.cis co.com/secu rity/center/	H-CIS-SPA1- 170523/855
CVSS Scoring S	Scale 0-1	L-2 2-3	<b>3-4 4-5 5-6</b> Page <b>444</b> of <b>1106</b>	6-7 7-	8 8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			SPA112 2-Port Phone Adapters could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to a missing authentication process within the firmware upgrade function. An attacker could exploit this vulnerability by upgrading an affected device to a crafted version of firmware. A successful exploit could allow the attacker to execute arbitrary code on the affected device with full privileges. Cisco has not released firmware updates to address this vulnerability. <b>CVE ID : CVE-2023- 20126</b>	content/Cisc oSecurityAd visory/cisco- sa-spa- unauth- upgrade- UqhyTWW	
Vendor: Dli					
Product: di					
Affected Ver	sion(s): a1				
Buffer Copy without Checking Size of Input ('Classic	02-May-2023	9.8	** UNSUPPORTED WHEN ASSIGNED ** D-Link DIR-868L Hardware version A1, firmware version 1.12 is vulnerable to Buffer Overflow. The	https://ww w.dlink.com/ en/security- bulletin/, https://supp ortannounce ment.us.dlin	H-DLI-DIR 170523/856

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			vulnerability is in scandir.sgi binary. CVE ID : CVE-2023- 29856	k.com/anno uncement/p ublication.as px?name=SA P10325	
Product: dir	-879			I	
Affected Ver	sion(s): a1				
Improper Authentica tion	01-May-2023	7.5	D-Link DIR-879 v105A1 is vulnerable to Authentication Bypass via phpcgi. CVE ID : CVE-2023- 30061	https://ww w.dlink.com/ en/security- bulletin/	H-DLI-DIR 170523/857
Product: dir	·-890l				
Affected Ver	sion(s): a1				
Improper Authentica tion	01-May-2023	7.5	D-Link DIR-890L FW1.10 A1 is vulnerable to Authentication bypass. <b>CVE ID : CVE-2023-</b> <b>30063</b>	https://ww w.dlink.com/ en/security- bulletin/	H-DLI-DIR 170523/858
Vendor: ez-	net		L	I	L
Product: ne	xt-7004n				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	6.1	A vulnerability was found in NEXTU NEXT-7004N 3.0.1. It has been classified as problematic. Affected is an unknown function of the file /boafrm/formFilter of the component POST Request Handler. The manipulation of the argument url with the input <svg< td=""><td>N/A</td><td>H-EZNEXT- 170523/859</td></svg<>	N/A	H-EZNEXT- 170523/859

0-1

1-2

**2-3** 3-4 4-5 Page **446** of **1106**  7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			onload=alert(1337)> leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB- 228012. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.		
			CVE ID : CVE-2023- 2521		
Vendor: feiy	uxing				
Product: ve					
Affected Ver	sion(s): -		A lassel: literat	E.	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	04-May-2023	7.2	A vulnerability was found in Chengdu VEC40G 3.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /send_order.cgi?para meter=access_detect of the component Network Detection. The manipulation of the argument COUNT with the input 3   netstat -an leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The	N/A	H-FEI-VEC4- 170523/860

0-1

1-2

**2-3** 3-4 4-5 Page **447** of **1106**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier VDB- 228013 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.		
			CVE ID : CVE-2023- 2522		
Vendor: fiio					
Product: me	5				
Affected Ver	sion(s): -				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	7.8	A buffer overflow in the component /proc/ftxxxx-debug of FiiO M6 Build Number v1.0.4 allows attackers to escalate privileges to root. <b>CVE ID : CVE-2023-</b> <b>30257</b>	N/A	H-FII-M6- 170523/861
Vendor: gar	0			<u> </u>	•
Product: wa	llbox_glb				
Affected Ver	sion(s): -				
Incorrect Permission Assignmen t for Critical Resource	04-May-2023	8.1	Insecure permissions in the settings page of GARO Wallbox GLB/GTB/GTC before v189 allows attackers to redirect users to a crafted update package link via a man-in-the- middle attack. <b>CVE ID : CVE-2023-</b> <b>30399</b>	N/A	H-GAR-WALL- 170523/862
Product: wa	llbox_gtb				
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>448</b> of <b>1106</b>	6-7 7-6	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Ver	Affected Version(s): -							
Incorrect Permission Assignmen t for Critical Resource	04-May-2023	8.1	Insecure permissions in the settings page of GARO Wallbox GLB/GTB/GTC before v189 allows attackers to redirect users to a crafted update package link via a man-in-the- middle attack. <b>CVE ID : CVE-2023-</b>	N/A	H-GAR-WALL- 170523/863			
			30399					
Product: wa								
Affected Ver	sion(s): -		L-	Γ				
Incorrect Permission Assignmen t for Critical Resource	04-May-2023	8.1	Insecure permissions in the settings page of GARO Wallbox GLB/GTB/GTC before v189 allows attackers to redirect users to a crafted update package link via a man-in-the- middle attack. <b>CVE ID : CVE-2023-</b> 20200	N/A	H-GAR-WALL- 170523/864			
Vondor: gl i	not		30399					
Vendor: gl-i Product: gl-								
Affected Ver								
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	02-May-2023	9.8	GL.iNET MT3000 4.1.0 Release 2 is vulnerable to OS Command Injection via /usr/lib/oui- httpd/rpc/logread. CVE ID : CVE-2023- 29778	N/A	H-GLGL-M- 170523/865			

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')					
Vendor: H3	C			1	
Product: gr	-1200w				
Affected Ver	sion(s): -				
Out-of- bounds Write	08-May-2023	9.8	H3C GR-1200W MiniGRW1A0V100R 006 was discovered to contain a stack overflow via the function set_tftp_upgrad. CVE ID : CVE-2023- 29693	N/A	H-H3C-GR-1- 170523/866
Out-of- bounds Write	08-May-2023	9.8	H3C GR-1200W MiniGRW1A0V100R 006 was discovered to contain a stack overflow via the function version_set. <b>CVE ID : CVE-2023-</b> <b>29696</b>	N/A	H-H3C-GR-1- 170523/867
Vendor: HP	1				
Product: in	tegrated_lights-	out			
Affected Ver	sion(s): 6				
N/A	01-May-2023	6.8	A potential security vulnerability has been identified in HPE ProLiant RL300 Gen11 Server. The vulnerability could result in the system being vulnerable to exploits by attackers with physical access inside the server chassis.	https://supp ort.hpe.com/ hpesc/public /docDisplay? docLocale=e n_US&docId =hpesbhf044 72en_us	H-HP-INTE- 170523/868

0-1

1-2

**2-3** 3-4 4-5 Page **450** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 28092		
Product: pr	oliant_rl300			• •	
Affected Ver	sion(s): gen_11				
N/A	01-May-2023	6.8	A potential security vulnerability has been identified in HPE ProLiant RL300 Gen11 Server. The vulnerability could result in the system being vulnerable to exploits by attackers with physical access inside the server chassis.	https://supp ort.hpe.com/ hpesc/public /docDisplay? docLocale=e n_US&docId =hpesbhf044 72en_us	H-HP-PROL- 170523/869
Vendor: IBN	Л		CVE ID : CVE-2023- 28092		
Product: 39					
Affected Ver					
Allecteu vei			A vulnorability in the		
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X- Force ID: 246320. <b>CVE ID : CVE-2023-</b> 24958	https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24632 0, https://ww w.ibm.com/s upport/page s/node/698 0845	H-IBM-3948- 170523/870

0-1

1-2

2-33-44-5Page 451 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 39	57-vec			L	
Affected Ver	sion(s): -				
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X- Force ID: 246320.	https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24632 0, https://ww w.ibm.com/s upport/page s/node/698 0845	H-IBM-3957- 170523/871
<b>D</b>			CVE ID : CVE-2023- 24958		
Product: 39					
Affected Ver	sion(s): - 04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X- Force ID: 246320. <b>CVE ID : CVE-2023-</b>	https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24632 0, https://ww w.ibm.com/s upport/page s/node/698 0845	H-IBM-3957- 170523/872
Vendor: Ler			24958		
	iovo iart_clock_essen	tial with	alaya huilt in		
i i ouucti sill	141 t_01001x_03301				

0-1

1-2

2-33-44-5Page 452 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Ver	Affected Version(s): -							
N/A	01-May-2023	8.8	A default password was reported in Lenovo Smart Clock Essential with Alexa Built In that could allow unauthorized device access to an attacker with local network access. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 113714	H-LEN-SMAR- 170523/873			
			0896					
	inkagile_hx1021							
Affected Ver	sion(s): -							
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/874			
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/875			
Product: th	Product: thinkagile_hx1320							
Affected Ver								
		Allected Version(s)						

0-1

1-2

2-33-44-5Page 453 of 1106

5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/876
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/877
			25492		
	inkagile_hx1321	L			
Affected Ver			A valid,		
N/A	01-May-2023	8.8	authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/878
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/879

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			behavior through a format string injection vulnerability in a web interface API.					
			CVE ID : CVE-2023- 25492					
Product: thi	inkagile_hx1331	_			I			
Affected Ver	sion(s): -							
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/880			
			CVE ID : CVE-2023- 0683					
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/881			
			CVE ID : CVE-2023- 25492					
	Product: thinkagile_hx1520-r							
Affected Ver	sion(s): -			https://supp				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/882			

 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
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/883
			CVE ID : CVE-2023- 25492		
	inkagile_hx1521	-r			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/884
			CVE ID : CVE-2023- 0683	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/885

0-1

1-2

**2-3** 3-4 4-5 Page **456** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx232(	)-е			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/886
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/887
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx2321	L			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/888
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	H-LEN-THIN- 170523/889

0-1

1-2

**2-3** 3-4 4-5 Page **457** of **1106**  6-7

7-8

8-9

Controlled Format Stringmay be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. CVE ID : CVE-2023- 25492m/us/en/pr oduct securi ty/LEN- 99936Product: thinkagile_tx2330Affected Version(s): -N/A01-May-20238.8A valid, authenticated API call. CVE ID : CVE-2023- 0683CVE ID : CVE-2023- 0683Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated API call. CVE ID : CVE-2023- 0683CVE ID : CVE-2023- 068301-May-20238.8A valid, authenticated API call. cvice of the XCC web user interface or other undefined behavior through a gerifically crated API call. CVE ID : CVE-2023- 0683Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. CVE ID : CVE-2023- 0936Product: thinkagile_tx231Product: thinkagile_tx233Kaffected Version(s): -	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Version(s): -N/A01-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN-99936H-LEN-THIN-170523/890Use of Externally-Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.https://supp oduct_securi ty/LEN-99936Product: tututational triangle_hx2318.8CVE ID : CVE-2023-25492https://supp oduct_securi ty/LEN-99936	Format			trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	oduct_securi ty/LEN-				
N/A01-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/890Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. CVE ID : CVE-2023- 25492https://supp ort.lenovo.co 	Product: thi	inkagile_hx2330	)			<u> </u>			
N/A01-May-20238.8authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/890Use of Externally Controlled Format String1-May-2023A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or ofter undefined behavior through a service of the XCC web user interface or ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/890Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or ofter undefined behavior through a web interface API.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936Use of Externally- Controlled Format String8.8Externally- commute trigger a denial of service of the XCC web user interface or ort.lenove.co m/us/en/pr oduct_securi ty/LEN- 99936H-LEN-THIN- trigger 3/2012Use of Externally- String01-May-20238.8Externally- commute trigger 3/2012H-LEN-THIN- trigger 3/2012Use of Externally- String01-May-20238.8Externally- commute trigger 3/2012H-LEN-THIN- trigger 3/2012Use of Externally- String01-May-20238.8Externally- commute trigger 3/2012H-LEN-THIN- trigger 3/2012Use of Externally- String01-May-2023 <td>Affected Ver</td> <td>sion(s): -</td> <td></td> <td></td> <td></td> <td></td>	Affected Ver	sion(s): -							
Use of Externally Ontrolled Formatof 1-May-20238.8authenticated user may be able to trigger a denial of service of the XCC other undefined behavior through a format string injection vulnerability in a web interface API.https://supp oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/891Product: th:tagile_hx2312	N/A	01-May-2023	8.8	authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	ort.lenovo.co m/us/en/pr oduct_securi ty/LEN-				
Product: thinkagile_hx2331	Externally- Controlled Format	01-May-2023	8.8	authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a	ort.lenovo.co m/us/en/pr oduct_securi ty/LEN-				
Affected Version(s): -	Product: thi	Product: thinkagile_hx2331							
	Affected Ver	sion(s): -							

0-1

1-2

**2-3** 3-4 4-5 Page **458** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/892
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/893
			25492		
	inkagile_hx272(	)-е			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/894
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/895

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inkagile_hx3320	)					
Affected Ver	sion(s): -						
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/896		
			CVE ID : CVE-2023- 0683				
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/897		
			CVE ID : CVE-2023- 25492				
Product: thinkagile_hx3321							
Affected Ver	sion(s): -			https://s			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/898		

CVSS Scoring Scale 3-4 4-5 5-6 6-7 0-1 1-2 2-3 7-8 Page 460 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/899
			CVE ID : CVE-2023- 25492		
	inkagile_hx3330				
Affected Ver	sion(s): -				_
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/900
			CVE ID : CVE-2023- 0683	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/901

0-1

1-2

2-33-44-5Page 461 of 1106

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx3331	Ĺ		L	
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/902
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/903
			25492		
Product: thi	inkagile_hx3375	5			I
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/904
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	H-LEN-THIN- 170523/905

0-1

1-2

**2-3** 3-4 4-5 Page **462** of **1106**  8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936			
Product: thi	inkagile_hx3376	5					
Affected Ver	sion(s): -						
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/906		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/907		
			25492				
Product: thinkagile_hx3520-g							
Affected Ver	sion(s): -						

0-1

1-2

**2-3** 3-4 4-5 Page **463** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/908
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/909
			CVE ID : CVE-2023- 25492		
	inkagile_hx3521	l-g			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/910
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/911

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inkagile_hx3720	)			I		
Affected Ver	sion(s): -						
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/912		
			0683				
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/913		
			CVE ID : CVE-2023- 25492				
Product: thinkagile_hx3721							
Affected Ver	sion(s): -						
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/914		

 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
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/915
			CVE ID : CVE-2023- 25492		
	inkagile_hx5520				
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/916
			CVE ID : CVE-2023- 0683	77750	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/917

0-1

1-2

**2-3** 3-4 4-5 Page **466** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx552(	)-с			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/918
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/919
			25492		
Product: thi	inkagile_hx5521	l			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/920
Use of Externally-	01-May-2023	8.8	<b>0683</b> A valid, authenticated user	https://supp ort.lenovo.co	H-LEN-THIN- 170523/921

0-1

1-2

**2-3** 3-4 4-5 Page **467** of **1106**  6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b> <b>25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936	
Product: thi	inkagile_hx5521	-C			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/922
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/923
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx5530				
Affected Ver	sion(s): -				

0-1

1-2

**2-3** 3-4 4-5 Page **468** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/924
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/925
			25492		
	inkagile_hx5531	L			
Affected Ver	sion(s): -		A valid,		
N/A	01-May-2023	8.8	authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/926
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/927

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inkagile_hx7520	)			I		
Affected Ver	sion(s): -						
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/928		
			CVE ID : CVE-2023- 0683				
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/929		
			CVE ID : CVE-2023- 25492				
Product: thinkagile_hx7521							
Affected Ver	sion(s): -			1			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/930		

 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
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/931
			CVE ID : CVE-2023- 25492		
	inkagile_hx7530				
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/932
			CVE ID : CVE-2023- 0683	77750	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/933

0-1

1-2

2-33-44-5Page 471 of 1106

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx7531	Ĺ		L	
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/934
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/935
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx782(	)			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/936
Use of Externally-	01-May-2023	8.8	<b>0683</b> A valid, authenticated user	https://supp ort.lenovo.co	H-LEN-THIN- 170523/937

0-1

1-2

2-33-44-5Page 472 of 1106

6-7

7-8

8-9

Controlled Format String			may be able to trigger a denial of service of the XCC	m/us/en/pr oduct_securi			
			web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	ty/LEN- 99936			
Product: thin	kagile_hx7821						
Affected Version	on(s): -						
N/A (	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/938		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/939		
			25492				
Product: thinkagile_hx_enclosure							
Affected Version	on(s): -						

0-1

1-2

2-3

3-44-5Page 473 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/940
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/941
			25492		
	inkagile_mx102	0			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/942
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/943

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inkagile_mx102	1_on_se3	50	<u> </u>	I		
Affected Ver	sion(s): -						
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/944		
			CVE ID : CVE-2023- 0683				
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/945		
			CVE ID : CVE-2023- 25492				
Product: thinkagile_mx3330-f							
Affected Ver	sion(s): -			1			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/946		

 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
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/947
			CVE ID : CVE-2023- 25492		
	inkagile_mx333	0-h			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/948
			CVE ID : CVE-2023- 0683	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/949

0-1

1-2

**2-3** 3-4 4-5 Page **476** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2023- 25492							
Product: thi	Product: thinkagile_mx3331-f									
Affected Ver	sion(s): -									
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/950					
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/951					
			CVE ID : CVE-2023- 25492							
Product: thi	inkagile_mx333	1-h			<u> </u>					
Affected Ver	sion(s): -									
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/952					
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	H-LEN-THIN- 170523/953					

0-1

1-2

**2-3** 3-4 4-5 Page **477** of **1106**  6-7

7-8

8-9

Format StringImage: StringImage: StringIm	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Version(s): -N/A01-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.https://supp oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/954Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or ofter undefined behavior through a myeb interface API.https://supp oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/954Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or ofter undefined behavior through a format string injection vulnerability in a web interface API.H-LEN-THIN- 170523/955Product: thikagile_mx353U_fVer ID : CVE-2023- 25492Ver ID : CVE-2023- 25492H-LEN-THIN- 170523/955	Controlled Format String			trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	oduct_securi ty/LEN-				
N/A01-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 9936H-LEN-THIN- 170523/954Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. CVE ID : CVE-2023- 25492https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 9936H-LEN-THIN- 170523/954VISE of Externally- 	Product: thi	inkagile_mx353	0-h						
N/A01-May-20238.8authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683https://supp oduct_securi y/LEN- 99936H-LEN-THIN- 170523/954Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/954Product: titute: trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936Product: titute: trigger adenial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936Product: titute: totalEXEMPTION (CVE ID : CVE-2023- 25492https://supp	Affected Ver	sion(s): -							
Use of Externally- Controlled Format String01-May-20238.8authenticated user may be able to trigger a denial of service of the XCC other undefined behavior through a format string injection vulnerability in a web interface API.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/955Product: tbitkagile_mx353/2	N/A	01-May-2023	8.8	authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	ort.lenovo.co m/us/en/pr oduct_securi ty/LEN-				
Product: thinkagile_mx3530_f	Use of Externally- Controlled Format String	01-May-2023	8.8	authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a	ort.lenovo.co m/us/en/pr oduct_securi ty/LEN-				
Affected Version(s): -	Product: thi	Product: thinkagile_mx3530_f							
	Affected Ver	sion(s): -							

0-1

1-2

**2-3** 3-4 4-5 Page **478** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/956
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/957
		-	25492		
	inkagile_mx353	1-f			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/958
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/959

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inkagile_mx353	1_h	I				
Affected Ver	sion(s): -						
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/960		
			CVE ID : CVE-2023- 0683				
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/961		
			CVE ID : CVE-2023- 25492				
Product: thinkagile_vx1320							
Affected Ver	sion(s): -			1			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/962		

CVSS Scoring Scale 3-4 4-5 5-6 6-7 0-1 1-2 2-3 7-8 Page 480 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/963
			CVE ID : CVE-2023- 25492		
	inkagile_vx2320				
Affected Ver	sion(s): -				_
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/964
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/965

0-1

1-2

2-33-44-5Page 481 of 1106

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_vx2330	•			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/966
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/967
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_vx3320	)			<u> </u>
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/968
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	H-LEN-THIN- 170523/969

0-1

1-2

**2-3** 3-4 4-5 Page **482** of **1106**  6-7

7-8

8-9

Format StringImage: StringImage: StringIm	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): -N/A01-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/970Use of Externally- Controlled Format01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or ofter undefined behavior through a format string injection vulnerability in a web interface API. CVE ID : CVE-2023- 25492https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/970Product: tbitkagile_vx3318.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. CVE ID : CVE-2023- 25492H-LEN-THIN- 170523/971Product: tbitkagile_vx331EA valid, authenticated API access may be able to to the through a format string injection vulnerability in a web interface API.	Controlled Format String			trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	oduct_securi ty/LEN-			
N/A01-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.https://supp oduct_securi ty/LEN- 9936H-LEN-THIN- 170523/970Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. CVE ID : CVE-2023- 25492https://supp oduct_securi ty/LEN- 9936H-LEN-THIN- 170523/970Product: tbitkagile_vx331A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or 	Product: thi	inkagile_vx3330	)					
N/A01-May-20238.8authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.https://supp oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/970Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a mulerability in a web interface API.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936Product: tritation trideCVE ID : CVE-2023- 25492Product tritation tritation	Affected Ver	sion(s): -						
Use of Externally Controlled Format String01-May-20238.8authenticated user may be able to trigger a denial of service of the XCC other undefined behavior through a format string injection vulnerability in a web interface API.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/971Product: thikagile_vx3331EVE ID : CVE-2023- 25492StringStringString	N/A	01-May-2023	8.8	authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	ort.lenovo.co m/us/en/pr oduct_securi ty/LEN-			
Product: thinkagile_vx3331	Use of Externally- Controlled Format String	01-May-2023	8.8	authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a	ort.lenovo.co m/us/en/pr oduct_securi ty/LEN-			
Affected Version(s): -	Product: thinkagile_vx3331							
	Affected Ver	sion(s): -						

0-1

1-2

**2-3** 3-4 4-5 Page **483** of **1106**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/972
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/973
			CVE ID : CVE-2023- 25492		
	inkagile_vx3520	-g			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/974
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/975

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			behavior through a format string injection vulnerability in a web interface API.					
			CVE ID : CVE-2023- 25492					
Product: thi	inkagile_vx3530	)-g	<u> </u>					
Affected Ver	sion(s): -							
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/976			
			CVE ID : CVE-2023- 0683					
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/977			
			CVE ID : CVE-2023- 25492					
	Product: thinkagile_vx3720							
Affected Ver	sion(s): -							
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/978			

 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
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/979
			CVE ID : CVE-2023- 25492		
	inkagile_vx5520				
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/980
			CVE ID : CVE-2023- 0683	77750	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/981

0-1

1-2

**2-3** 3-4 4-5 Page **486** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_vx5530				
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/982
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/983
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_vx7320	_n			<u> </u>
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/984
Use of Externally-	01-May-2023	8.8	<b>0683</b> A valid, authenticated user	https://supp ort.lenovo.co	H-LEN-THIN- 170523/985

0-1

1-2

**2-3** 3-4 4-5 Page **487** of **1106**  6-7

7-8

8-9

Controlled Format								
String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936				
Product: thin	kagile_vx7330							
Affected Version	on(s): -							
N/A (	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/986			
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/987			
			CVE ID : CVE-2023- 25492					
Product: thinkagile_vx7520								
Affected Version	on(s): -							

0-1

1-2

**2-3** 3-4 4-5 Page **488** of **1106**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/988
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/989
			CVE ID : CVE-2023- 25492		
	inkagile_vx7520	<u>_n</u>			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/990
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/991

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API.		
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_vx7530	)			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/992
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/993
			CVE ID : CVE-2023- 25492		
	inkagile_vx7531				
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/994

 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
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/995
			CVE ID : CVE-2023- 25492		
	inkagile_vx7820				
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/996
			CVE ID : CVE-2023- 0683	77750	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/997

0-1

1-2

2-33-44-5Page 491 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_vx_1se				
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/998
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/999
			CVE ID : CVE-2023- 25492		
Product: th	inkagile_vx_2u4	n			
Affected Ver	0				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1000
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	H-LEN-THIN- 170523/1001

0-1

1-2

2-33-44-5Page 492 of 1106

6-7

7-8

8-9

Controlled Format Stringmay be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API CVE ID : CVE-2023- 25492m/us/en/pr oduct.securi y/LEN- 9936Product: thinkagile_vx_4uA valid, authenticated AVIC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683https://supp ort.lenovo.co m/us/en/pr oduct.securi ty/LEN- 9936H-LEN-THIN- 170523/1002N/A01-May-20238.8A valid, authenticated API crafted API call. CVE ID : CVE-2023- 0683https://supp ort.lenovo.co m/us/en/pr oduct.securi ty/LEN- 9936H-LEN-THIN- 170523/1002Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vuberability in a web interface API. CVE ID : CVE-2023- 25492H-LEN-THIN- 170523/1002Product: thinkedge_se450_ Z5492CVE ID : CVE-2023- 25492https://suppProduct: thinkedge_se450_ CVE ID : CVE-2023-H-LEN-THIN- 170523/1003	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): -N/A01-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 9936H-LEN-THIN- 170523/1002Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or ofter undefined behavior through a format string injection vulnerability in a web interface API. CVE ID : CVE-2023- 25492H-LEN-THIN- 170523/1002Product: tbitkedge_se450.8.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. CVE ID : CVE-2023- 25492H-LEN-THIN- 170523/1003Product: tbitkedge_se450.EventUse of cve interface API.H-LEN-THIN- 170523/1003	Format			trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	oduct_securi ty/LEN-			
N/A01-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.https://supp oduct_securi ty/LEN- 9936H-LEN-THIN- 170523/1002Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.https://supp oduct_securi ty/LEN- 9936H-LEN-THIN- 170523/1002Product: tbitkedge_se450:8.8CVE ID : CVE-2023- 25492https://supp 	Product: thi	inkagile_vx_4u						
N/A01-May-20238.8authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.https://sup oduct_securi y/LEN- 99936H-LEN-THIN- 170523/1002Use of Externally Controlled Format String1-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or ofter undefined behavior through a service of the XCC web user interface or ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936NA Product.securi ty/LEN- 99936Use of Externally- Controlled Format String01-May-20238.8Research authenticated user may be able to trigger a denial of service of the XCC web user interface or ofter undefined behavior through a web interface API.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936Use of Externally- Controlled Format String8.8Research authenticated user may be able to trigger a denial of service of the XCC web user interface or ofter undefined behavior through a web interface API.https://supp oduct_securi ty/LEN- 99936Use of Externally- CVE ID : CVE-2023- 25492CVE ID : CVE-2023- comatorhttps://supp oduct_securi ty/LEN- securiceProduct:Use of CVE ID : CVE-2023- comatorProduct use of the typehttps://suppProduct:Use of CVE ID : CVE-2023- comatorProduct use of typeProduct:Use of typeProduct use of typeProduct use of typeProduct:Use of type <td< td=""><td>Affected Ver</td><td>sion(s): -</td><td></td><td></td><td></td><td></td></td<>	Affected Ver	sion(s): -						
Use of Externally- Controlled Format String01-May-20238.8authenticated user may be able to trigger a denial of service of the XCC other undefined behavior through a format string injection vulnerability in a web interface API.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/1003Product: th:kedge_se450-	N/A	01-May-2023	8.8	authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	ort.lenovo.co m/us/en/pr oduct_securi ty/LEN-			
Product: thinkedge_se450_	Externally- Controlled Format	01-May-2023	8.8	authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a	ort.lenovo.co m/us/en/pr oduct_securi ty/LEN-			
Affected Version(s): -	Product: thinkedge_se450_							
	Affected Ver	sion(s): -						

0-1

1-2

**2-3** 3-4 4-5 Page **493** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1004
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1005
			CVE ID : CVE-2023- 25492		
	inkstation_p920				
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1006
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1007

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inksystem_sd53	0	L				
Affected Ver	sion(s): -						
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1008		
			CVE ID : CVE-2023- 0683				
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1009		
			CVE ID : CVE-2023- 25492				
Product: thinksystem_sd630_v2							
Affected Ver	sion(s): -			https://supp			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1010		

 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
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1011
			CVE ID : CVE-2023- 25492		
	inksystem_sd65	0			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1012
			CVE ID : CVE-2023- 0683	<i></i>	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1013

0-1

1-2

**2-3** 3-4 4-5 Page **496** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inksystem_sd65	0-n_v2			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1014
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1015
			25492		
Product: thi	inksystem_sd65	0_v2		·	
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1016
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	H-LEN-THIN- 170523/1017

0-1

1-2

**2-3** 3-4 4-5 Page **497** of **1106**  6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b> <b>25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936			
Product: thi	nksystem_se35	0					
Affected Ver	sion(s): -						
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1018		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1019		
			25492				
Product: thinksystem_sn550							
Affected Ver	sion(s): -						

0-1

1-2

**2-3** 3-4 4-5 Page **498** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1020
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1021
			25492		
	inksystem_sn55	0_v2			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1022
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1023

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inksystem_sn85	0	<u> </u>		I		
Affected Ver	sion(s): -						
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1024		
			CVE ID : CVE-2023- 0683				
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1025		
			CVE ID : CVE-2023- 25492				
Product: thinksystem_sr150							
Affected Ver	sion(s): -						
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1026		

 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
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1027
			CVE ID : CVE-2023- 25492		
	inksystem_sr15	8			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1028
			CVE ID : CVE-2023- 0683	77750	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1029

0-1

1-2

2-33-44-5Page 501 of 1106

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inksystem_sr25	0			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1030
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1031
			CVE ID : CVE-2023- 25492		
Product: thi	inksystem_sr25	0_v2			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1032
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	H-LEN-THIN- 170523/1033

0-1

1-2

2-33-44-5Page 502 of 1106

6-7

7-8

8-9

Format StringImage: StringImage: StringIm	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Version(s): -N/A01-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/1034Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. CVE ID : CVE-2023- 25492H-LEN-THIN- 170523/1034Product: tbitksystem_sr258_v2VStringhttps://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	Controlled Format String			trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	oduct_securi ty/LEN-			
N/A01-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.https://supp oduct_securi ty/LEN- 9936H-LEN-THIN- 170523/1034Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. CVE ID : CVE-2023- 25492https://supp oduct_securi ty/LEN- 9936H-LEN-THIN- 170523/1034VISE of Externally- Controlled Format01-May-20238.8A valid, authenticated user may be able to 	Product: thi	inksystem_sr25	8					
N/A01-May-20238.8authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/1034Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/1034Product: titusystem_sr252/20238.8Externally- cyte ID : CVE-2023- 25492https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/1035	Affected Ver	sion(s): -						
Use of Externally- Controlled Format String01-May-20238.8authenticated user may be able to trigger a denial of service of the XCC other undefined behavior through a format string injection vulnerability in a web interface API.https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936H-LEN-THIN- 170523/1035Product: thicksystem_sr258-v2	N/A	01-May-2023	8.8	authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	ort.lenovo.co m/us/en/pr oduct_securi ty/LEN-			
Product: thinksystem_sr258_v2	Use of Externally- Controlled Format String	01-May-2023	8.8	authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a	ort.lenovo.co m/us/en/pr oduct_securi ty/LEN-			
Affected Version(s): -	Product: thinksystem_sr258_v2							
	Affected Ver	sion(s): -						

0-1

1-2

**2-3** 3-4 4-5 Page **503** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1036
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1037
		0	25492		
Affected Ver	inksystem_sr53	0			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1038
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1039

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inksystem_sr55	0	L				
Affected Ver	sion(s): -						
N/A	01-May-2023	01-May-2023 8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1040		
			CVE ID : CVE-2023- 0683				
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1041		
			CVE ID : CVE-2023- 25492				
Product: thinksystem_sr570							
Affected Ver	sion(s): -						
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1042		

CVSS Scoring Scale 0-1 1-2 2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1043
			CVE ID : CVE-2023- 25492		
	inksystem_sr59	0			
Affected Ver	sion(s): -				_
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1044
			CVE ID : CVE-2023- 0683	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1045

0-1

1-2

**2-3** 3-4 4-5 Page **506** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inksystem_sr63	0			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1046
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1047
			25492		
	inksystem_sr63	0_v2			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1048
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	H-LEN-THIN- 170523/1049

0-1

1-2

**2-3** 3-4 4-5 Page **507** of **1106**  6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936				
Product: thi	inksystem_sr64	5		<u> </u>				
Affected Ver	sion(s): -							
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1050			
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1051			
			CVE ID : CVE-2023- 25492					
Product: thi	Product: thinksystem_sr645_v3							
Affected Ver	sion(s): -							

0-1

1-2

**2-3** 3-4 4-5 Page **508** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1052
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1053
			25492		
	inksystem_sr65	0			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1054
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1055

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inksystem_sr65	0_v2			I		
Affected Ver	sion(s): -						
N/A	01-May-2023	01-May-2023 8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1056		
			CVE ID : CVE-2023- 0683	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1057		
			CVE ID : CVE-2023- 25492				
Product: thinksystem_sr665							
Affected Ver	sion(s): -			1			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1058		

 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
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1059
			CVE ID : CVE-2023- 25492		
	inksystem_sr66	5_v3			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1060
			CVE ID : CVE-2023- 0683	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1061

0-1

1-2

2-33-44-5Page 511 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inksystem_sr67	0			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1062
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1063
			25492		
Product: thi	inksystem_sr67	0_v2			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1064
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	H-LEN-THIN- 170523/1065

0-1

1-2

2-33-44-5Page 512 of 1106

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b> <b>25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936	
Product: thi	nksystem_sr85	0			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1066
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1067
			25492		
Product: thi	nksystem_sr85	0p			l 
Affected Ver	sion(s): -				

0-1

1-2

2-33-44-5Page 513 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1068
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1069
			25492		
	inksystem_sr85	0_v2			
Affected Ver	sion(s): -		A -1:1		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1070
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1071

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			behavior through a format string injection vulnerability in a web interface API.					
			CVE ID : CVE-2023- 25492					
Product: thi	inksystem_sr86	0						
Affected Ver	sion(s): -							
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1072			
			CVE ID : CVE-2023- 0683	55530				
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1073			
			CVE ID : CVE-2023- 25492					
	Product: thinksystem_sr860_v2							
Affected Ver	sion(s): -			1				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1074			

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

 Page 515 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1075
			CVE ID : CVE-2023- 25492		
	inksystem_sr95	0			
Affected Ver	sion(s): -				
N/A	01-May-2023	01-May-2023 8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1076
			CVE ID : CVE-2023- 0683	77750	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1077

0-1

1-2

2-33-44-5Page 516 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2023- 25492							
Product: thi	Product: thinksystem_st250									
Affected Ver	sion(s): -									
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1078					
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1079					
			25492							
	inksystem_st25	0_v2								
Affected Ver	sion(s): -			1						
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1080					
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	H-LEN-THIN- 170523/1081					

0-1

1-2

2-33-44-5Page 517 of 1106

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b> <b>25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936				
Product: thi	inksystem_st258	3						
Affected Ver	sion(s): -							
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1082			
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1083			
			CVE ID : CVE-2023- 25492					
Product: thi	Product: thinksystem_st258_v2							
Affected Ver	sion(s): -							

0-1

1-2

**2-3** 3-4 4-5 Page **518** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1084
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1085
			CVE ID : CVE-2023- 25492		
	inksystem_st550	)			
Affected Ver	sion(s): -				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1086
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1087

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inksystem_st650	)_v2	I				
Affected Ver	sion(s): -						
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1088		
			CVE ID : CVE-2023- 0683	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1089		
			CVE ID : CVE-2023- 25492				
Product: thinksystem_st658_v2							
Affected Ver	sion(s): -			https://s			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1090		

 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
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	H-LEN-THIN- 170523/1091
			CVE ID : CVE-2023- 25492		
Vendor: mil	_				
Product: nc					
Affected Ver	sion(s): -				
N/A	08-May-2023	7.5	Milesight NCR/camera version 71.8.0.6-r5 discloses sensitive information through an unspecified request.	N/A	H-MIL-NCR\- 170523/1092
			CVE ID : CVE-2023- 24505		
Insufficient ly Protected Credentials	08-May-2023	7.5	Milesight NCR/camera version 71.8.0.6-r5 exposes credentials through	N/A	H-MIL-NCR\- 170523/1093

0-1

1-2

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			an unspecified request.					
			CVE ID : CVE-2023- 24506					
Vendor: mit								
	t-2741gnac-n2							
Affected Ver	sion(s): -		Mit - OPT					
N/A	05-May-2023	8.8	MitraStar GPT- 2741GNAC-N2 with firmware BR_g5.9_1.11(WVK.0) )b32 was discovered to contain a remote code execution (RCE) vulnerability in the ping function. <b>CVE ID : CVE-2023-</b> <b>30065</b>	N/A	H-MIT-GPT 170523/1094			
Vendor: Qua	alcomm							
	5_5g_iot_moden	n						
Affected Vers	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-315 170523/1095			
Product: 8905								
Affected Ver	sion(s): -							
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa	H-QUA-8905- 170523/1096			
CVSS Scoring S	Scale 0-1 :	1-2 2-3	<b>3 3-4 4-5 5-6</b> Page <b>522</b> of <b>1106</b>	6-7 7-8	8 8-9 <mark>9-10</mark>			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Conversion or Cast			CVE ID : CVE-2023- 21665	ny/product- security/bull etins/may- 2023- bulletin					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-8905- 170523/1097				
Product: 89	09								
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-8909- 170523/1098				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-8909- 170523/1099				
Product: 89	17								
Affected Ver	Affected Version(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-8917- 170523/1100				

0-1

1-2

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-8917- 170523/1101		
Product: 89	52						
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-8952- 170523/1102		
Product: 89	53						
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-8953- 170523/1103		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-8953- 170523/1104		
	Product: 8953pro       Affected Version(s): -						

0-1

1-2

**2-3** 3-4 4-5 Page **524** of **1106**  6-7 7-8

5-6

Conversion				https://ww			
or Cast	)2-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-8953- 170523/1105		
Missing Release of Memory after Effective Lifetime	)2-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-8953- 170523/1106		
Product: 8956	6						
Affected Versio	on(s): -						
Incorrect Type Conversion or Cast	)2-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-8956- 170523/1107		
Product: 8976	б						
Affected Versio	on(s): -						
Incorrect Type Conversion or Cast	)2-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-8976- 170523/1108		
Product: 8976pro							
Affected Versio	Affected Version(s): -						

0-1

1-2

2-33-44-5Page 525 of 1106

5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-8976- 170523/1109		
Product: 89	98						
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-8998- 170523/1110		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-8998- 170523/1111		
Product: 92	06_lte_modem						
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-9206- 170523/1112		
Product: apq5053-aa							
Affected Ver	sion(s): -						

0-1

1-2

**2-3** 3-4 4-5 Page **526** of **1106**  6-7 7-8

5-6

Incorrect Type Conversion or Cast0.2-May-20237.8Memory corruption in Graphics while afile. CVE ID : CVE-2023- 2023- builetinhttps://ww w.qualcomm com/compa ny/product- security/buil etins/may- 2023- builetinH-QUA-APQ5- 170523/1113Missing Release of Memory after Effective0.2-May-20237.8Memory Corruption after allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm com/compa ny/product- security/buil etins/may- 2023- builetinH-QUA-APQ5- 170523/1114Product aperotrIntervertMemory Corruption after allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm com/compa ny/product- security/buil etins/may- 2023- builetinH-QUA-APQ5- 170523/1114Incorrect Type Conversion or Cast0.2-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 2023- builetinhttps://ww w.qualcomm com/compa ny/product- security/buil etins/may- 2023- builetinH-QUA-APQ8- 170523/1115Product aperotre Type Conversion or Cast0.2-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 2023- builetinhttps://ww w.qualcomm com/compa ny/product- security/buil etins/may- 2023- builetinIncorrect Type Conversion or Cast0.2-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 2023- builetinhttps://ww w.qualcomm com/compa ny/product- security/bui	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Missing Release of Memory after Effective Lifetime0.2 - May-20237.8Intentory of unpuol in Graphics while alcocated through the graphics pool. CVE ID : CVE-2023- 21666w.qualcomm .com/compa ny/product- security/bull etins/may- 2023 - bulletinH-QUA-APQ5- 170523/1114Product: apy8017Affected Version(s): -Memory corruption in Graphics while inporting a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023 - bulletinH-QUA-APQ8- 170523/1114Product: apy8052Froduct: apy8052Mittps://ww conversion or Cast0.2 - May-2023 0.2 - May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023 - bulletinH-QUA-APQ8- 170523/1115Froduct: apy8052Product: apy8053-aa7.8Memory corruption in Graphics while importing a file. CONversion or Casthttps://ww v.qualcomm .com/compa ny/product- security/bull etins/may- 2023 - bulletinH-QUA-APQ8- 170523/1116Product: apy8052- Conversion or Cast0.2 - May-20237.8Memory corruption in Graphics while importing a file. CVE-2023- 21665https://ww v.qualcomm .com/compa ny/product- security/bull etins/may- 2023 - bulletinH-QUA-APQ8- 170523/1116Product: apy8052- Conversion or Cast0.2 - May-20237.8Memory	Type Conversion	02-May-2023	7.8	in Graphics while importing a file. <b>CVE ID : CVE-2023-</b>	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-			
Affected Version(s): -Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinH-QUA-APQ8- 170523/1115Product: apq8052Affected Version(s): -Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. CC Product: apq8052https://ww w.qualcomm .com/compa ny/product- 	Release of Memory after Effective	02-May-2023	7.8	in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b>	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-			
Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023:</b> <b>21665</b> https://ww w.qualcomm .om/compa ny/product- security/bull etins/may- 2023- bulletinH-QUA-APQ8- 170523/1115Product: apertor Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023:</b> <b>DII</b> https://ww w.qualcomm .om/compa ny/product- security/bull etins/may- 2023- bulletinH-QUA-APQ8- 170523/1115Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023:</b> 	Product: ap	q8017						
Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinH-QUA-APQ8- 170523/1115Product: security/bull etins/may- 2023- bulletinMemory corruption in Graphics while in G	Affected Ver	sion(s): -						
Affected Version(s): -Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b> https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinH-QUA-APQ8- 170523/1116 <b>Product: arysense</b>	Type Conversion	02-May-2023	7.8	in Graphics while importing a file. <b>CVE ID : CVE-2023-</b>	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-			
Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b> https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinH-QUA-APQ8- 170523/1116Product: apg8053-aa <th bit="" column="" in="" of="" security="" security<="" td="" the=""><td>Product: ap</td><td>q8052</td><td></td><td></td><td></td><td></td></th>	<td>Product: ap</td> <td>q8052</td> <td></td> <td></td> <td></td> <td></td>	Product: ap	q8052					
Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinH-QUA-APQ8- 170523/1116Product: apg8053-aa7.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 2023- bulletinH-QUA-APQ8- 170523/1116	Affected Ver	sion(s): -						
	Type Conversion	02-May-2023	7.8	in Graphics while importing a file. <b>CVE ID : CVE-2023-</b>	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-	• •		
Affected Version(s): -								
	Affected Ver	Affected Version(s): -						

0-1

1-2

2-33-44-5Page 527 of 1106

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-APQ8- 170523/1117
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-APQ8- 170523/1118
Product: ap	q8053-ac				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-APQ8- 170523/1119
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-APQ8- 170523/1120
Product: ap	q8053-lite				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-APQ8- 170523/1121
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5-6 Page <b>528</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-APQ8- 170523/1122
Product: ap	-				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-APQ8- 170523/1123
Product: ap	q8064au			I	L
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-APQ8- 170523/1124
Product: ap	q8076				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	H-QUA-APQ8- 170523/1125

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID						
				2023- bulletin							
Product: aq	Product: aqt1000										
Affected Vers	sion(s): -										
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	.com/compa ny/product- security/bull	H-QUA-AQT1- 170523/1126						
Product: ar	8031										
Affected Ver	sion(s): -										
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	.com/compa ny/product- security/bull	H-QUA-AR80- 170523/1127						
Product: ar	8035			· ·							
Affected Ver	sion(s): -										
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	.com/compa ny/product- security/bull	H-QUA-AR80- 170523/1128						
Product: c-v	/2x_9150										
Affected Ver	sion(s): -										
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	w.qualcomm .com/compa	H-QUA-C-V2- 170523/1129						
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	Descripti	ion & CVE	ID	Patch		NCIIF	PC ID		
						2023- oulletin					
Product: cs	Product: csra6620										
Affected Ver	sion(s): -										
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory ( in Graphi importing <b>CVE ID :</b> ( <b>21665</b>	cs while g a file.	on v .« 23- 23-	nttps://w w.qualcom com/com ny/produ ecurity/k etins/may 2023- pulletin	nm pa ct- pull	H-QUA-0 170523/			
Product: cs	ra6640										
Affected Ver	sion(s): -										
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory of in Graphi importing CVE ID : 0 21665	cs while g a file.	on v .« 23- 22-	nttps://w w.qualcom com/com ny/produ security/k etins/may 2023- pulletin	nm pa ct- pull	H-QUA-0 170523/			
Product: cs	rb31024										
Affected Ver	sion(s): -										
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory of in Graphi importing CVE ID : 0 21665	cs while g a file.	on v  23- 2	nttps://w w.qualcom com/com ny/produ ecurity/k etins/may 2023- pulletin	nm pa ct- pull	H-QUA-0 170523/			
Product: flig	ght_rb5_5g_pla	tform									
Affected Ver	sion(s): -										
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory of in Graphi importing CVE ID : 0 21665	cs while g a file.	23- x v  r s	nttps://w v.qualcom com/com ny/produ recurity/k etins/may	nm pa ct- pull	H-QUA-F 170523/			
CVSS Scoring S											

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-FLIG- 170523/1134
Product: hon	ne_hub_100_pla	atform			
Affected Versi	ion(s): -				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-HOME- 170523/1135
Product: md	m9250				
Affected Versi	ion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-MDM9- 170523/1136
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-MDM9- 170523/1137
Product: md	m9628				

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-MDM9- 170523/1138
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-MDM9- 170523/1139
Product: mo	lm9650				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-MDM9- 170523/1140
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-MDM9- 170523/1141
Product: ms	sm8108				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-MSM8- 170523/1142
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>533</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-MSM8- 170523/1143
Product: ms					
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-MSM8- 170523/1144
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-MSM8- 170523/1145
Product: ms	sm8608			L	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-MSM8- 170523/1146

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-MSM8- 170523/1147
Product: ms	sm8909w				
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-MSM8- 170523/1148
Product: ms	sm8996au				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-MSM8- 170523/1149
Product: qa	m8295p				
Affected Ver	sion(s): -				
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. CVE ID : CVE-2023- 21642	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QAM8- 170523/1150

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Descriptio	on & CVE	ID	Patch		NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory of in Graphic importing CVE ID : C 21665	cs while g a file.	on 3-	https://ww w.qualcomn .com/compa ny/product- security/bu etins/may- 2023- bulletin	n a -	H-QUA-QAM8- 170523/1151
Product: qc	a-4020-0-217m	sp						
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory of in Graphic importing CVE ID : C 21665	cs while g a file.	on 3-	https://ww w.qualcomn .com/compa ny/product- security/but etins/may- 2023- bulletin	n a -	H-QUA-QCA 170523/1152
Product: qc	a-4020-1-217m	sp						
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory of in Graphic importing CVE ID : C 21665	cs while g a file.	on 3-	https://ww w.qualcomn .com/compa ny/product- security/bu etins/may- 2023- bulletin	n a -	H-QUA-QCA 170523/1153
Product: qc	a-4024-0-68cm	qfn						
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory of in Graphic importing CVE ID : C 21665	cs while g a file.	on 3-	https://ww w.qualcomn .com/compa ny/product- security/bu etins/may- 2023- bulletin	n a -	H-QUA-QCA 170523/1154
Product: qc	a-4024-1-68cm	qfn						
Affected Version(s): -								
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4	4-5	5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA 170523/1155
Product: qc					
Affected Ver	sion(s): -				_
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1156
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1157
Product: qc	a6174a				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1158
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-QCA6- 170523/1159

0-1

1-2

**2-3** 3-4 4-5 Page **537** of **1106**  6-7 7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin	
Product: qca	a6310				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1160
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1161
Product: qca	a6320				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1162
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1163
Product: qca	a6335				

0-1

1-2

**2-3** 3-4 4-5 Page **538** of **1106**  5-6

6-7 7-8

NCIIPC ID
n a - H-QUA-QCA6- ll 170523/1164
n a - H-QUA-QCA6- ll 170523/1165
n a - H-QUA-QCA6- ll 170523/1166
n a - H-QUA-QCA6- ll 170523/1167
n H-QUA-QCA6- a 170523/1168

Page 539 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1169
Product: qc	a6420				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1170
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1171
Product: qc	a6421				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1172

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1173
Product: qc	a6426				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1174
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1175
Product: qc	a6430				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1176
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-QCA6- 170523/1177

0-1

1-2

2-33-44-5Page 541 of 1106

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin	
Product: qca	a6431				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1178
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1179
Product: qca	a6436				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1180
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1181
Product: qca	a6564				

0-1

1-2

2-33-44-5Page 542 of 1106

5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Descriptio	on & CVE I	D	Patch		NCIIP	C ID
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory co in Graphic importing CVE ID : C 21665	s while a file.	n 3-	https://w w.qualcom .com/com ny/produ security/h etins/may 2023- bulletin	nm pa ct- oull	H-QUA-Q 170523/	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory C in Graphic accessing a allocated t graphics p CVE ID : C 21666	s while a buffer chrough t oool.	the 3-	https://w w.qualcon .com/com ny/produ security/k etins/may 2023- bulletin	nm pa ct- oull	H-QUA-Q 170523/	
Product: qc	a6564a								
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory co in Graphic importing CVE ID : C 21665	s while a file.	n 3-	https://w w.qualcon .com/com ny/produ security/h etins/may 2023- bulletin	nm pa ct- oull	H-QUA-Q 170523/	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory C in Graphic accessing a allocated t graphics p CVE ID : C 21666	s while a buffer hrough t ool.	the 3-	https://w w.qualcon .com/com ny/produ security/k etins/may 2023- bulletin	nm pa ct- oull	H-QUA-Q 170523/	•
Product: qc	a6564au				·				
Affected Ver	sion(s): -								
Incorrect Type	02-May-2023	7.8	Memory co in Graphic importing	s while	11	https://w w.qualcon .com/com ny/produ	nm pa	H-QUA-Q 170523/	
CVSS Scoring S	Scale 0-1	1-2 2-3	3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Page 543 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1187
Product: qc	a6574				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1188
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1189
Product: qc	a6574a				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1190

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1191
Product: qc	a6574au				
Affected Ver	sion(s): -				
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1192
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1193
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1194
Product: qc					
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-QCA6- 170523/1195
CVSS Scoring S	Scale 0-1 1	1-2 2-3	3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Page 545 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21665	etins/may- 2023- bulletin	
Product: qc	a6595				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1196
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1197
Product: qc	a6595au				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1198
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1199
Product: qc	a6696				

0-1

1-2

**2-3** 3-4 4-5 Page **546** of **1106**  5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Affected Ver	sion(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1200	
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1201	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1202	
Product: qc	a6698aq			<u> </u>		
Affected Ver	sion(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA6- 170523/1203	
Product: qca8081						
Affected Ver	sion(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa	H-QUA-QCA8- 170523/1204	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page <b>547</b> of <b>1106</b>										

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			CVE ID : CVE-2023- 21665	ny/product- security/bull etins/may- 2023- bulletin	
Product: qc	a8337				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA8- 170523/1205
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA8- 170523/1206
Product: qc	a9367				<u> </u>
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA9- 170523/1207
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA9- 170523/1208

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qc	a9377				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA9- 170523/1209
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA9- 170523/1210
Product: qc	a9379				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA9- 170523/1211
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCA9- 170523/1212
Product: qc	m2290			I	
Affected Ver	sion(s): -				

0-1

1-2

**2-3** 3-4 4-5 Page **549** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCM2- 170523/1213
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCM2- 170523/1214
Product: qc	m4290				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCM4- 170523/1215
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCM4- 170523/1216
Product: qc	m6125				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-QCM6- 170523/1217
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>550</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCM6- 170523/1218
Product: qc	m6490				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCM6- 170523/1219
Product: qc	n6024			I	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCN6- 170523/1220
Product: qc	n9011				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	H-QUA-QCN9- 170523/1221

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCN9- 170523/1222
Product: qc	n9012				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCN9- 170523/1223
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCN9- 170523/1224
Product: qc	n9024				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCN9- 170523/1225
Product: qc	n9074				
Affected Ver	sion(s): -				

0-1

1-2

2-33-44-5Page 552 of 1106

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCN9- 170523/1226
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCN9- 170523/1227
Product: qc	s2290				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS2- 170523/1228
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS2- 170523/1229
Product: qc	s400				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-QCS4- 170523/1230
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>553</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may- 2023- bulletin	
Product: qc	s410				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS4- 170523/1231
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS4- 170523/1232
Product: qc	s4290			I	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS4- 170523/1233
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS4- 170523/1234
Product: qc	s605				

0-1

1-2

**2-3** 3-4 4-5 Page **554** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS6- 170523/1235
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS6- 170523/1236
Product: qc	s610			L	
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS6- 170523/1237
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS6- 170523/1238
Product: qc	s6125			I	
Affected Vers	sion(s): -				
Incorrect	02-May-2023	7.8	Memory corruption in Graphics while	https://ww w.qualcomm .com/compa	H-QUA-QCS6- 170523/1239

Page 555 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS6- 170523/1240
Product: qc	s6490				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS6- 170523/1241
Product: qc	s8155				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS8- 170523/1242
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS8- 170523/1243

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Product: qc	Product: qcs8250								
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS8- 170523/1244				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QCS8- 170523/1245				
Product: qn	1215								
Affected Ver	sion(s): -								
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QM21- 170523/1246				
Product: qr	b5165								
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QRB5- 170523/1247				
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://ww w.qualcomm	H-QUA-QRB5- 170523/1248				

 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
Memory after Effective Lifetime			accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	.com/compa ny/product- security/bull etins/may- 2023- bulletin	
Product: qr					
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QRB5- 170523/1249
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QRB5- 170523/1250
Product: qr	b5165n				1
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QRB5- 170523/1251
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	H-QUA-QRB5- 170523/1252
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5-6 Page <b>558</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Page 558 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023- bulletin	
Product: qs	m8250				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QSM8- 170523/1253
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-QSM8- 170523/1254
Product: sa	4150p			<u> </u>	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA41- 170523/1255
Product: sa	4155p				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA41- 170523/1256

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sad	6145p			L	
Affected Vers	sion(s): -				
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA61- 170523/1257
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA61- 170523/1258
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA61- 170523/1259
Product: sat	6150p				
Affected Vers	sion(s): -				
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA61- 170523/1260
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-SA61- 170523/1261
CVSS Scoring S	icale 0-1	L-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- 21665	etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA61- 170523/1262
Product: sa					
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA61- 170523/1263
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA61- 170523/1264
Product: sa	6155p				
Affected Ver	sion(s): -				
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA61- 170523/1265

0-1

1-2

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA61- 170523/1266
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA61- 170523/1267
Product: sa	<u> </u>				
Affected Ver	sion(s): -			1	
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA81- 170523/1268
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA81- 170523/1269
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	H-QUA-SA81- 170523/1270

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023- bulletin	
Product: sa	8150p				
Affected Ver	sion(s): -				
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. CVE ID : CVE-2023- 21642	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA81- 170523/1271
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA81- 170523/1272
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA81- 170523/1273
Product: sa	8155				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA81- 170523/1274
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://ww w.qualcomm	H-QUA-SA81- 170523/1275

 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
Memory after Effective Lifetime			accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	.com/compa ny/product- security/bull etins/may- 2023- bulletin	
Product: sa	8155p				
Affected Ver	sion(s): -				
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. CVE ID : CVE-2023- 21642	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA81- 170523/1276
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA81- 170523/1277
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA81- 170523/1278
Product: sa	8195p				
Affected Ver	sion(s): -				
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address.	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	H-QUA-SA81- 170523/1279

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID : CVE-2023- 21642	2023- bulletin		
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA81- 170523/1280	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA81- 170523/1281	
Product: sa8295p						
Affected Ver	sion(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA82- 170523/1282	
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA82- 170523/1283	
Product: sa	8540p			I		
Affected Ver	sion(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory	https://ww w.qualcomm	H-QUA-SA85- 170523/1284	

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

Product: sd626         Affected Version(s):         Incorrect         Type         Conversion         or Cast         Missing         Release of         Memory	- y-2023		management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	.com/compa ny/product- security/bull etins/may- 2023- bulletin		
Affected Version(s):N/A02-MayProduct: sd-26Affected Version(s):Affected Version(s):Incorrect Type Conversion or CastMissing Release of Memory after Effective Lifetime						
N/A 02-May Product: sd Affected Version (s): Incorrect Type Conversion or Cast Missing Release of Memory after Effective Lifetime						
Product: sd=26 Affected Version(s): Incorrect Type Conversion or Cast Missing Release of Memory after Effective Lifetime	y-2023					
Affected Version(s):Incorrect Type Conversion or Cast02-MayMissing Release of Memory after Effective Lifetime02-May		7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SA90- 170523/1285	
Incorrect Type Conversion or Cast Missing Release of Memory after Effective Lifetime						
Type Conversion or Cast02-MayMissing Release of Memory after Effective Lifetime02-May	-					
Release of Memory after Effective Lifetime	y-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD62- 170523/1286	
Product: sd660	y-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD62- 170523/1287	
	Product: sd660					
Affected Version(s):	-					
Incorrect 02-May Type		7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product-	H-QUA-SD66- 170523/1288	
CVSS Scoring Scale	y-2023	1-2 2-3				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD66- 170523/1289
Product: sd	670				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD67- 170523/1290
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD67- 170523/1291
Product: sd	675				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD67- 170523/1292

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD67- 170523/1293
Product: sd	730				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD73- 170523/1294
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD73- 170523/1295
Product: sd	835				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD83- 170523/1296
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-SD83- 170523/1297

0-1

1-2

**2-3** 3-4 4-5 Page **568** of **1106**  6-7 7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin	
Product: sd	855				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD85- 170523/1298
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD85- 170523/1299
Product: sd	865_5g				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD86- 170523/1300
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD86- 170523/1301
Product: sd	888				

0-1

1-2

**2-3** 3-4 4-5 Page **569** of **1106**  5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Ver	Affected Version(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD88- 170523/1302		
Product: sd	a\/sdm845			L			
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDA\- 170523/1303		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDA\- 170523/1304		
Product: sd	m429			I			
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDM4- 170523/1305		
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer	https://ww w.qualcomm .com/compa ny/product-	H-QUA-SDM4- 170523/1306		

0-1

1-2

2-33-44-5Page 570 of 1106

6-7

5-6

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			allocated through the graphics pool. CVE ID : CVE-2023- 21666	security/bull etins/may- 2023- bulletin	
Product: sd	m429w				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDM4- 170523/1307
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDM4- 170523/1308
Product: sd	m439				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDM4- 170523/1309
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDM4- 170523/1310

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Product: sd	Product: sdm450						
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDM4- 170523/1311		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDM4- 170523/1312		
Product: sd	m660						
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDM6- 170523/1313		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDM6- 170523/1314		
Product: sd	m670						
Affected Ver	sion(s): -						

0-1

1-2

2-3

3-44-5Page 572 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDM6- 170523/1315
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDM6- 170523/1316
Product: sd	m710				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDM7- 170523/1317
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDM7- 170523/1318
Product: sd	m845				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-SDM8- 170523/1319
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>573</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDM8- 170523/1320
Product: sd					
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDX2- 170523/1321
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDX2- 170523/1322
Product: sd	x55			<u> </u>	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDX5- 170523/1323

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SDX5- 170523/1324				
Product: sd_675									
Affected Version(s): -									
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD_6- 170523/1325				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SD_6- 170523/1326				
Product: sm4125									
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM41- 170523/1327				
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-SM41- 170523/1328				

0-1

1-2

2-33-44-5Page 575 of 1106

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin					
Product: sm4250-aa									
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM42- 170523/1329				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM42- 170523/1330				
Product: sm	14350			<u> </u>					
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM43- 170523/1331				
Product: sm	Product: sm4350-ac								
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	H-QUA-SM43- 170523/1332				

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023- bulletin	
Product: sm	14375				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM43- 170523/1333
Product: sm	6115			I	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM61- 170523/1334
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM61- 170523/1335
Product: sm	6125			I	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM61- 170523/1336

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM61- 170523/1337
Product: sm	6150				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM61- 170523/1338
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM61- 170523/1339
Product: sm	16150-ac				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM61- 170523/1340
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-SM61- 170523/1341

0-1

1-2

**2-3** 3-4 4-5 Page **578** of **1106**  6-7 7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin	
Product: sm	6225				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM62- 170523/1342
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM62- 170523/1343
Product: sm	6225-ad				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM62- 170523/1344
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM62- 170523/1345
Product: sm	6250				

0-1

1-2

**2-3** 3-4 4-5 Page **579** of **1106**  5-6

6-7 7-8

	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM62- 170523/1346
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM62- 170523/1347
Product: sm	6250p				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM62- 170523/1348
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM62- 170523/1349
Product: sm	6350			I	I
Affected Vers	sion(s): -				
	02-May-2023	7.8	Memory corruption in Graphics while	https://ww w.qualcomm .com/compa	H-QUA-SM63- 170523/1350

Page 580 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM63- 170523/1351
Product: sm	16375				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM63- 170523/1352
Product: sm	7125				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM71- 170523/1353
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM71- 170523/1354

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Product: sm	Product: sm7150-aa							
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM71- 170523/1355			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM71- 170523/1356			
Product: sm	7150-ab							
Affected Vers	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM71- 170523/1357			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM71- 170523/1358			
Product: sm Affected Vers								

0-1

1-2

**2-3** 3-4 4-5 Page **582** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM71- 170523/1359		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM71- 170523/1360		
Product: sm	-						
Affected Ver	sion(s): -				1		
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM72- 170523/1361		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM72- 170523/1362		
Product: sm	17250-aa						
Affected Ver	sion(s): -						
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-SM72- 170523/1363		
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10           Page 583 of 1106         Page 583 of 1106							

Page **583** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin	
Product: sm	17250-ab				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM72- 170523/1364
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM72- 170523/1365
Product: sm	17250-ac			I	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM72- 170523/1366
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM72- 170523/1367
Product: sm	17250p				

0-1

1-2

**2-3** 3-4 4-5 Page **584** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Ver	Affected Version(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM72- 170523/1368		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM72- 170523/1369		
Product: sm	7315						
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM73- 170523/1370		
Product: sm	17325						
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM73- 170523/1371		
Product: sm	17325-ae			·			
Affected Ver	sion(s): -						

0-1

1-2

**2-3** 3-4 4-5 Page **585** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM73- 170523/1372			
Product: sm	17325-af							
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM73- 170523/1373			
Product: sm	17325p							
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM73- 170523/1374			
Product: sm	17350-ab							
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM73- 170523/1375			
Product: sm	Product: sm8150							
Affected Ver	Affected Version(s): -							
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b>	5 6-7 7-8	8 8-9 9-10			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM81- 170523/1376
Product: sm	18150-ac				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM81- 170523/1377
Product: sm	18250				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM82- 170523/1378
Product: sm	18250-ab				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM82- 170523/1379
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://ww w.qualcomm	H-QUA-SM82- 170523/1380

 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
Memory after Effective Lifetime			accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	.com/compa ny/product- security/bull etins/may- 2023- bulletin	
Product: sm					
Affected Ver	sion(s): -			1	
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM82- 170523/1381
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM82- 170523/1382
Product: sm	18350		L	I	L
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SM83- 170523/1383
Product: sm	18350-ac			L	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product-	H-QUA-SM83- 170523/1384

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin	
Product: sn	apdragon_1200	wearabl	e_platform		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1385
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1386
Product: sn	apdragon_208_p	processor		L	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1387
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1388

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Descriptio	on & CVE II	D	Patch	NCIIPC ID	)
Product: sna	apdragon_630_r	nobile_pl	atform					
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory of in Graphic importing CVE ID : 0 21665	cs while g a file.	n ;-	https://ww w.qualcomm .com/compa ny/product- security/bul etins/may- 2023- bulletin	H-QUA-SNA	
Product: sna	apdragon_632_1	nobile_pl	atform					
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory of in Graphic importing CVE ID : C 21665	cs while g a file.	n 3-	https://ww w.qualcomm .com/compa ny/product- security/bul etins/may- 2023- bulletin	H-QUA-SNA	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory ( in Graphic accessing allocated graphics p CVE ID : ( 21666	cs while a buffer through thoool.	he S-	https://ww w.qualcomm .com/compa ny/product- security/bul etins/may- 2023- bulletin	H-QUA-SNA	
Product: sna	apdragon_636_r	nobile_pl	atform					
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory of in Graphic importing CVE ID : C 21665	cs while g a file.	n }-	https://ww w.qualcomm .com/compa ny/product- security/bul etins/may- 2023- bulletin	H-QUA-SNA	
Product: snapdragon_7c\+_gen_3_compute								
Affected Ver	sion(s): -							
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4	4-5	5-6	6-7	7-8 8-9 9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1393
Product: sn	apdragon_820_a	utomotiv	/e_platform		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1394
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1395
Product: sn	apdragon_auto_	4g_mode	m		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1396
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-SNAP- 170523/1397

0-1

1-2

2-33-44-5Page 591 of 1106

6-7 7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin				
Product: sn	apdragon_auto_	5g_mode	m-rf					
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1398			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1399			
Product: sn	apdragon_w5\+	_gen_1_w	earable_platform					
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1400			
Product: sn	apdragon_wear	_2100_pla	atform					
Affected Ver	Affected Version(s): -							
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	H-QUA-SNAP- 170523/1401			
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				
				2023- bulletin					
Product: sn	Product: snapdragon_wear_2500_platform								
Affected Ver	sion(s): -								
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1402				
Product: sn	apdragon_wear	_3100_pla	atform	L					
Affected Ver	sion(s): -								
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1403				
Product: sn	apdragon_wear_	_4100\+_	platform						
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1404				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1405				

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sn	apdragon_x12_l	te_moder	n	I	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1406
Product: sn	apdragon_x20_l	te_moder	n		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1407
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1408
Product: sn	apdragon_x24_l	te_moder	n		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1409
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://ww w.qualcomm	H-QUA-SNAP- 170523/1410

 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	
Memory after Effective Lifetime			accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	.com/compa ny/product- security/bull etins/may- 2023- bulletin		
Product: sn	apdragon_x50_5	g_moden	n-rf_system		I	
Affected Ver	sion(s): -				-	
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1411	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1412	
Product: sn	apdragon_x55_5	g_moden	n-rf_system		I	
Affected Ver	sion(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1413	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	H-QUA-SNAP- 170523/1414	
CVSS Scoring Scale       0-1       1-2       2-3       3-4       4-5       5-6       6-7       7-8       8-9       9-10						

Page 595 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				2023- bulletin				
Product: sn	apdragon_x5_lte	e_modem						
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1415			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1416			
Product: sn	apdragon_x65_5	g_moden	n-rf_system	I				
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1417			
Product: sn	apdragon_xr1_p	latform						
Affected Ver	Affected Version(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1418			

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1419
	apdragon_xr2\+	_gen_1_p	latform		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1420
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1421
Product: sna	apdragon_xr2_5	g_platfor	m		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SNAP- 170523/1422
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-SNAP- 170523/1423

0-1

1-2

**2-3** 3-4 4-5 Page **597** of **1106**  8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin		
Product: ssi	m7250-aa					
Affected Ver	sion(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SSM7- 170523/1424	
Product: sw	5100					
Affected Ver	sion(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SW51- 170523/1425	
Product: sw	5100p					
Affected Ver	sion(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SW51- 170523/1426	
Product: sx	r1120					
Affected Version(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-SXR1- 170523/1427	
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10	
			Page <b>598</b> of <b>1106</b>			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21665	etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SXR1- 170523/1428
Product: sx	r2130				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SXR2- 170523/1429
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-SXR2- 170523/1430
Product: wo	:d9326			I	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1431

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1432
Product: wo					
Affected Ver	sion(s): -				1
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1433
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1434
Product: wo	:d9335				L
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1435
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-WCD9- 170523/1436

0-1

1-2

**2-3** 3-4 4-5 Page **600** of **1106**  5-6

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin	
Product: wo	d9340				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1437
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1438
Product: wo	d9341				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1439
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1440
Product: wo	d9370				

0-1

1-2

2-33-44-5Page 601 of 1106

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1441
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1442
Product: wo	d9371				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1443
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1444
Product: wo	:d9375			I	
Affected Ver	sion(s): -				
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product-	H-QUA-WCD9- 170523/1445
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5-6	6-7 7-8	8 8-9 <mark>9-10</mark>

Page 602 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Conversion or Cast			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1446				
Product: wo	:d9380								
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1447				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1448				
Product: wo	:d9385								
Affected Ver	Affected Version(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1449				

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCD9- 170523/1450
Product: wo					
Affected Ver	sion(s): -				Γ
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1451
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1452
Product: wo	m3615				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1453
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-WCN3- 170523/1454

0-1

1-2

**2-3** 3-4 4-5 Page **604** of **1106**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin	
Product: wc	m3620				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1455
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1456
Product: wc	m3660				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1457
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1458
Product: wc	m3660b			•	

0-1

1-2

**2-3** 3-4 4-5 Page **605** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Version(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1459			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1460			
Product: wo	cn3680							
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1461			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1462			
Product: wo	cn3680b							
Affected Ver	sion(s): -							
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product-	H-QUA-WCN3- 170523/1463			
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5-1	5 6-7 7-8	8 8-9 9-10			
CAPP SCOLING 2		1 2 2-3	J-4 4-3 J-1	-/ /-0	01-6 6-0			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1464
Product: wo	cn3910				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1465
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1466
Product: wo	m3950				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1467

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1468
Product: wo					
Affected Ver	sion(s): -				Γ
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1469
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1470
Product: wo	cn3988				L
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1471
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-WCN3- 170523/1472

0-1

1-2

**2-3** 3-4 4-5 Page **608** of **1106**  5-6

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin	
Product: wo	m3990				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1473
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1474
Product: wo	m3998			<u> </u>	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1475
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1476
Product: wo	cn3999				

0-1

1-2

**2-3** 3-4 4-5 Page **609** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1477		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN3- 170523/1478		
Product: wo	m6740						
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN6- 170523/1479		
Product: wo	m6750						
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN6- 170523/1480		
Product: wo	Product: wcn685x-1						
Affected Ver	Affected Version(s): -						

0-1

1-2

2-33-44-5Page 610 of 1106

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN6- 170523/1481
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN6- 170523/1482
Product: wo	cn685x-5				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN6- 170523/1483
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WCN6- 170523/1484
Product: ws	a8810				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull	H-QUA-WSA8- 170523/1485
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>611</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WSA8- 170523/1486
Product: ws					
Affected Ver	sion(s): -			1	
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WSA8- 170523/1487
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WSA8- 170523/1488
Product: ws	a8830				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WSA8- 170523/1489

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WSA8- 170523/1490
Product: ws	a8835				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WSA8- 170523/1491
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	H-QUA-WSA8- 170523/1492
Vendor: Roo	ckwellautomatio	on			
Product: arr	morstart_st_281	e			
Affected Vers	sion(s): -				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	7.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	H-ROC-ARMO- 170523/1493
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 613 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.		
			CVE ID : CVE-2023- 29030		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	7.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability. CVE ID : CVE-2023- 29031	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	H-ROC-ARMO- 170523/1494
Improper Neutralizat ion of Input During	11-May-2023	6.5	A cross site scripting vulnerability was discovered in Rockwell	https://rock wellautomati on.custhelp.c om/app/ans wers/answe	H-ROC-ARMO- 170523/1495

0-1

1-2

**2-3** 3-4 4-5 Page **614** of **1106**  8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Automation's ArmorStart ST product	r_view/a_id/ 1139438	
			A cross site scripting vulnerability was discovered that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.		
			29024		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	6.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	H-ROC-ARMO- 170523/1496

0-1

1-2

2-33-44-5Page 615 of 1106

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			required for successful exploitation of this vulnerability.		
			CVE ID : CVE-2023- 29023		
			A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	H-ROC-ARMO- 170523/1497
			CVE ID : CVE-2023- 29022		
Improper Neutralizat ion of	11-May-2023	5.9		https://rock wellautomati on.custhelp.c	H-ROC-ARMO- 170523/1498

0-1

1-2

3-4 2-3 4-5 Page 616 of 1106

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product	om/app/ans wers/answe r_view/a_id/ 1139438	
			that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.		
			CVE ID : CVE-2023- 29025		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	H-ROC-ARMO- 170523/1499
Scripting')			that could potentially allow a malicious user with admin		

0-1

1-2

2-33-44-5Page 617 of 1106

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.		
			CVE ID : CVE-2023- 29026		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	H-ROC-ARMO- 170523/1500

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29027		
			A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. CVE ID : CVE-2023- 29028	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	H-ROC-ARMO- 170523/1501
Improper Neutralizat ion of Input	11-May-2023	5.9	A cross site scripting vulnerability was discovered in	https://rock wellautomati on.custhelp.c om/app/ans	H-ROC-ARMO- 170523/1502

0-1

1-2

2-33-44-5Page 619 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Rockwell Automation's ArmorStart ST product	wers/answe r_view/a_id/ 1139438	
			that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. CVE ID : CVE-2023- 29029		
Product: ar	morstart_st_284	ee			
Affected Ver	sion(s): -				
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	7.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	H-ROC-ARMO- 170523/1503

0-1

1-2

**2-3** 3-4 4-5 Page **620** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.		
			CVE ID : CVE-2023- 29030		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	7.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability. CVE ID : CVE-2023- 29031	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	H-ROC-ARMO- 170523/1504
Improper Neutralizat ion of Input During Web Page	11-May-2023	6.5	A cross site scripting vulnerability was discovered in Rockwell Automation's	https://rock wellautomati on.custhelp.c om/app/ans wers/answe	H-ROC-ARMO- 170523/1505

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			ArmorStart ST product	r_view/a_id/ 1139438	
			A cross site scripting vulnerability was discovered that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.		
			CVE ID : CVE-2023- 29024		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	6.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	H-ROC-ARMO- 170523/1506

0-1

1-2

2-33-44-5Page 622 of 1106

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploitation of this vulnerability.		
			CVE ID : CVE-2023- 29023		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. CVE ID : CVE-2023- 29022	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	H-ROC-ARMO- 170523/1507
Improper Neutralizat ion of Input	11-May-2023	5.9	A cross site scripting vulnerability was	https://rock wellautomati on.custhelp.c om/app/ans	H-ROC-ARMO- 170523/1508

3-4

Page 623 of 1106

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
During Web Page Generation ('Cross-site Scripting')			discovered in Rockwell Automation's ArmorStart ST product	wers/answe r_view/a_id/ 1139438	
			that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. CVE ID : CVE-2023- 29025		
Improper Neutralizat ion of Input During Web Page Generation	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/	H-ROC-ARMO- 170523/1509
('Cross-site Scripting')			that could potentially allow a malicious user with admin privileges and network access to	1139438	

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.		
			CVE ID : CVE-2023- 29026		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	H-ROC-ARMO- 170523/1510

0-1

1-2

2-33-44-5Page 625 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29027		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. <b>CVE ID : CVE-2023- 29028</b>	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	H-ROC-ARMO- 170523/1511
Improper Neutralizat ion of Input During Web Page Generation	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	H-ROC-ARMO- 170523/1512

0-1

1-2

**2-3** 3-4 4-5 Page **626** of **1106**  5-6

6-7

7-8

8-9

('Cross-site Scripting')			ArmorStart ST product		
			that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.		
Vendor: Same	sung		CVE ID : CVE-2023- 29029		
Product: exyr	_				
Affected Versi					
Buffer Copy without Checking	04-May-2023	9.8	Potential buffer overflow vulnerability in auth api in mm_Authentication.c in Shannon baseband prior to SMR May- 2023 Release 1 allows remote attackers to cause invalid memory access. <b>CVE ID : CVE-2023- 21494</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	H-SAM-EXYN- 170523/1513
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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-May-2023	9.8	Potential buffer overflow vulnerability in mm_LteInterRatMan agement.c in Shannon baseband prior to SMR May- 2023 Release 1 allows remote attackers to cause invalid memory access. <b>CVE ID : CVE-2023-</b> <b>21503</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	H-SAM-EXYN- 170523/1514
Product: ex	ynos_1080				
Affected Ver	sion(s): -				
Improper Handling of Exceptiona l Conditions	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface. <b>CVE ID : CVE-2023- 29092</b>	https://semi conductor.sa msung.com/ support/qua lity- support/pro duct- security- updates/	H-SAM-EXYN- 170523/1515
Product: ex	-			•	
Affected Ver	sion(s): -				
Improper Handling of Exceptiona	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem	https://semi conductor.sa msung.com/ support/qua lity-	H-SAM-EXYN- 170523/1516

ÿ			_							
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
l Conditions			5123, Exynos Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface. <b>CVE ID : CVE-2023-</b> <b>29092</b>	support/pro duct- security- updates/	
Product: ex	ynos_5300				I
Affected Ver	sion(s): -				
Improper Handling of Exceptiona l Conditions	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface. <b>CVE ID : CVE-2023- 29092</b>	https://semi conductor.sa msung.com/ support/qua lity- support/pro duct- security- updates/	H-SAM-EXYN- 170523/1517
Product: ex	ynos_980				
Affected Ver					
Improper Handling of Exceptiona l Conditions	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos	https://semi conductor.sa msung.com/ support/qua lity- support/pro	H-SAM-EXYN- 170523/1518
CVSS Scoring S	Scale 0-1 C	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>629</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Page 629 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface. <b>CVE ID : CVE-2023-</b>	duct- security- updates/	
Vonder	machift		29092		
Vendor: sha	_				
Affected Ver					
Out-of- bounds Read	02-May-2023	5.7	Insufficient length checks in the ShapeShift KeepKey hardware wallet firmware before 7.7.0 allow a global buffer overflow via crafted messages. Flaws in cf_confirmExecTx() in ethereum_contracts. c can be used to reveal arbitrary microcontroller memory on the device screen or crash the device. With physical access to a PIN-unlocked device, attackers can extract the BIP39 mnemonic secret from the hardware wallet. <b>CVE ID : CVE-2023- 27892</b>	https://githu b.com/keepk ey/keepkey- firmware/pu ll/337	H-SHA-KEEP- 170523/1519

0-1

1-2

**2-3** 3-4 4-5 Page **630** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Sie	mens		I		I
Product: 6g	k1411-1ac00				
Affected Ver	sion(s): -				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	7.6	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to overwrite any file the Linux user `ccuser` has write access to, or to download any file the Linux user `ccuser` has read- only access to. <b>CVE ID : CVE-2023- 29104</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	H-SIE-6GK1- 170523/1520
Missing Standardiz ed Error Handling Mechanism	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	H-SIE-6GK1- 170523/1521

0-1

1-2

2-33-44-5Page 631 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device is vulnerable to a denial of service while parsing a random (non-JSON) MQTT payload. This could allow an attacker who can manipulate the communication between the MQTT broker and the affected device to cause a denial of service (DoS). <b>CVE ID : CVE-2023- 29105</b>		
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint is accessible via REST API without authentication. This could allow an unauthenticated remote attacker to download the files available via the endpoint.	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	H-SIE-6GK1- 170523/1522

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29106		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	09-May-2023	7.2	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The web based management of affected devices does not properly validate user input, making it susceptible to command injection. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges. <b>CVE ID : CVE-2023-</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	H-SIE-6GK1- 170523/1523
Files or Directories Accessible to External Parties	09-May-2023	5.3	28832 A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint discloses some undocumented files. This could allow an unauthenticated remote attacker to gain access to additional	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	H-SIE-6GK1- 170523/1524

0-1

1-2

2-33-44-5Page 633 of 1106

5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information resources.		
			CVE ID : CVE-2023- 29107		
Use of Hard- coded Password	09-May-2023	4.3	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device uses a hard-coded password to protect the diagnostic files. This could allow an authenticated attacker to access protected data. <b>CVE ID : CVE-2023- 29103</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	H-SIE-6GK1- 170523/1525
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	2.7	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	H-SIE-6GK1- 170523/1526

0-1

1-2

**2-3** 3-4 4-5 Page **634** of **1106**  6-7

7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to write any file with the extension `.db`. <b>CVE ID : CVE-2023-</b> <b>29128</b>		
Product: 6g	k1411-5ac00				
Affected Ver	rsion(s): -				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	7.6	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to overwrite any file the Linux user `ccuser` has write access to, or to download any file the Linux user `ccuser` has read- only access to.	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	H-SIE-6GK1- 170523/1527

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29104		
Missing Standardiz ed Error Handling Mechanism	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device is vulnerable to a denial of service while parsing a random (non-JSON) MQTT payload. This could allow an attacker who can manipulate the communication between the MQTT broker and the affected device to cause a denial of service (DoS). <b>CVE ID : CVE-2023- 29105</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	H-SIE-6GK1- 170523/1528
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	H-SIE-6GK1- 170523/1529

0-1

1-2

**2-3** 3-4 4-5 Page **636** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			export endpoint is accessible via REST API without authentication. This could allow an unauthenticated remote attacker to download the files available via the endpoint. <b>CVE ID : CVE-2023- 29106</b>		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	09-May-2023	7.2	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The web based management of affected devices does not properly validate user input, making it susceptible to command injection. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges. <b>CVE ID : CVE-2023- 28832</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	H-SIE-6GK1- 170523/1530
Files or Directories Accessible to External Parties	09-May-2023	5.3	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	H-SIE-6GK1- 170523/1531

0-1

1-2

**2-3** 3-4 4-5 Page **637** of **1106**  5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CC716 (All versions >= V2.0 < V2.1). The export endpoint discloses some undocumented files. This could allow an unauthenticated remote attacker to gain access to additional information resources. CVE ID : CVE-2023-		
Use of Hard- coded Password	09-May-2023	4.3	29107 A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device uses a hard-coded password to protect the diagnostic files. This could allow an authenticated attacker to access protected data. CVE ID : CVE-2023- 29103	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	H-SIE-6GK1- 170523/1532
Improper Limitation of a Pathname	09-May-2023	2.7	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All	https://cert- portal.sieme ns.com/prod uctcert/pdf/	H-SIE-6GK1- 170523/1533

0-1

1-2

**2-3** 3-4 4-5 Page **638** of **1106**  8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			<pre>versions &gt;= V2.0 &lt; V2.1), SIMATIC Cloud Connect 7 CC716 (All versions &gt;= V2.0 &lt; V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to write any file with the extension `.db`. CVE ID : CVE-2023- 29128</pre>	ssa- 555292.pdf	
Product: sca	alance_lpe9403				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	09-May-2023	9.9	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). The web based management of affected device does not properly validate user input, making it susceptible to command injection. This could allow an authenticated remote attacker to access the underlying operating system as the root user.	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 325383.pdf	H-SIE-SCAL- 170523/1534

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 27407		
Creation of Temporary File With Insecure Permission s	09-May-2023	3.3	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). The `i2c` mutex file is created with the permissions bits of `- rw-rw-rw-`. This file is used as a mutex for multiple applications interacting with i2c. This could allow an authenticated attacker with access to the SSH interface on the affected device to interfere with the integrity of the mutex and the data it protects. <b>CVE ID : CVE-2023- 27408</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 325383.pdf	H-SIE-SCAL- 170523/1535
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	3.3	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). A path traversal vulnerability was found in the `deviceinfo` binary via the `mac` parameter. This could allow an authenticated attacker with access to the SSH interface on the affected device to read the contents of any file named `address`.	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 325383.pdf	H-SIE-SCAL- 170523/1536

0-1

1-2

**2-3** 3-4 4-5 Page **640** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			CVE ID : CVE-2023- 27409				
Heap- based Buffer Overflow	09-May-2023	2.7	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). A heap-based buffer overflow vulnerability was found in the `edgebox_web_app` binary. The binary will crash if supplied with a backup password longer than 255 characters. This could allow an authenticated privileged attacker to cause a denial of service. <b>CVE ID : CVE-2023-</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 325383.pdf	H-SIE-SCAL- 170523/1537		
Vendor: Tei	nda		27410				
Product: ac							
Affected Ver	sion(s): -						
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	05-May-2023	9.8	Tenda AC18 v15.03.05.19(6318_) _cn was discovered to contain a command injection vulnerability via the deviceName parameter in the setUsbUnload function. <b>CVE ID : CVE-2023-</b>	https://githu b.com/Drizzl ingSun/Tend a/blob/main /AC18/8/8. md	H-TEN-AC18- 170523/1538		
Dura da da com	01		30135				
	Product: n301						
Affected Ver	51011(5): 0.0						

0-1

1-2

5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmissi on of Sensitive Informatio n	01-May-2023	5.7	Cleartext Transmission in set- cookie:ecos_pw: Tenda N301 v6.0, Firmware v12.02.01.61_multi allows an authenticated attacker on the LAN or WLAN to intercept communications with the router and obtain the password. <b>CVE ID : CVE-2023-</b> <b>29680</b>	N/A	H-TEN-N301- 170523/1539
Cleartext Transmissi on of Sensitive Informatio n	01-May-2023	5.7	Cleartext Transmission in cookie:ecos_pw: in Tenda N301 v6.0, firmware v12.03.01.06_pt allows an authenticated attacker on the LAN or WLAN to intercept communications with the router and obtain the password. <b>CVE ID : CVE-2023-</b> <b>29681</b>	N/A	H-TEN-N301- 170523/1540
Vendor: tot	olink				
Product: a7	100ru				
Affected Ver	sion(s): -				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS	05-May-2023	9.8	TOTOLINK A7100RU V7.4cu.2313_B20191 024 is vulnerable to Command Injection. <b>CVE ID : CVE-2023-</b> <b>30053</b>	N/A	H-TOT-A710- 170523/1541
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>
			Page <b>642</b> of <b>1106</b>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')					
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command	05-May-2023	9.8	TOTOLINK A7100RU V7.4cu.2313_B20191 024 has a Command Injection vulnerability. An attacker can obtain a stable root shell through a specially constructed payload. <b>CVE ID : CVE-2023-</b>	N/A	H-TOT-A710- 170523/1542
Injection')			30054		
Product: x5					
Affected Ver	sion(s): -			-	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	05-May-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B2020 1102 and V9.1.0u.6369_B2023 0113 contain a command insertion vulnerability in setting/setTracerout eCfg. This vulnerability allows an attacker to execute arbitrary commands through the "command" parameter. <b>CVE ID : CVE-2023-</b> <b>30013</b>	N/A	H-TOT-X500- 170523/1543
Vendor: Zyx					
Product: Nb	<b>с</b>				
Affected Ver	sion(s): v2				
Improper Neutralizat ion of Input During Web Page	01-May-2023	7.5	A cross-site scripting (XSS) vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0	https://ww w.zyxel.com /global/en/s upport/secu rity- advisories/z	H-ZYX-NBG 170523/1544
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')			could allow a remote authenticated attacker with administrator privileges to store malicious scripts using a web management interface parameter, resulting in denial- of-service (DoS) conditions on an affected device. <b>CVE ID : CVE-2023-</b> <b>22921</b>	yxel- security- advisory-for- multiple- vulnerabiliti es-in-nbg- 418n-v2- home-router	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-May-2023	7.5	A buffer overflow vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote unauthenticated attacker to cause DoS conditions by sending crafted packets if Telnet is enabled on a vulnerable device. <b>CVE ID : CVE-2023- 22922</b>	https://ww w.zyxel.com /global/en/s upport/secu rity- advisories/z yxel- security- advisory-for- multiple- vulnerabiliti es-in-nbg- 418n-v2- home-router	H-ZYX-NBG 170523/1545
Use of Externally- Controlled Format String	01-May-2023	6.5	A format string vulnerability in a binary of the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote authenticated attacker to cause denial-of-service	https://ww w.zyxel.com /global/en/s upport/secu rity- advisories/z yxel- security- advisory-for- multiple- vulnerabiliti es-in-nbg-	H-ZYX-NBG 170523/1546

0-1

1-2

**2-3** 3-4 4-5 Page **644** of **1106**  5-6

7-8

6-7

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			(DoS) conditions on an affected device. CVE ID : CVE-2023- 22923	418n-v2- home-router				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-May-2023	4.9	A buffer overflow vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote authenticated attacker with administrator privileges to cause denial-of-service (DoS) conditions by executing crafted CLI commands on a vulnerable device. <b>CVE ID : CVE-2023- 22924</b>	https://ww w.zyxel.com /global/en/s upport/secu rity- advisories/z yxel- security- advisory-for- multiple- vulnerabiliti es-in-nbg- 418n-v2- home-router	H-ZYX-NBG 170523/1547			
Product: nb								
Affected Ver	sion(s): -			1				
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	01-May-2023	8.8	The post- authentication command injection vulnerability in the Zyxel NBG6604 firmware version V1.01(ABIR.0)C0 could allow an authenticated attacker to execute some OS commands remotely by sending a crafted HTTP request. <b>CVE ID : CVE-2023- 22919</b>	https://ww w.zyxel.com /global/en/s upport/secu rity- advisories/z yxel- security- advisory-for- post- authenticatio n-command- injection- vulnerability -in-nbg6604- home-router	H-ZYX-NBG6- 170523/1548			
Operating System								
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>645</b> of <b>1106</b>	6-7 7-8	3 8-9 <mark>9-10</mark>			

Page 645 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Vendor: Adv	vantech								
Product: ek	Product: eki-1521_firmware								
Affected Ver	sion(s): * Up to (i	ncluding)	1.21						
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the NTP server input field, which can be triggered by authenticated users via a crafted POST request. CVE ID : CVE-2023- 2573	https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBL	O-ADV-EKI 170523/1549				
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the device name input field, which can be triggered by authenticated users via a crafted POST request. <b>CVE ID : CVE-2023- 2574</b>	https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBL	O-ADV-EKI 170523/1550				

0-1

1-2

**2-3** 3-4 4-5 Page **646** of **1106**  5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stack-based Buffer Overflow vulnerability, which can be triggered by authenticated users via a crafted POST request. <b>CVE ID : CVE-2023- 2575</b>	https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBL	O-ADV-EKI 170523/1551
	i-1522_firmwar				
Affected Ver	<mark>sion(s): * Up to (</mark> i	including)			
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the NTP server input field, which can be triggered by authenticated users via a crafted POST request. CVE ID : CVE-2023- 2573	https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBL	O-ADV-EKI 170523/1552
Improper Neutralizat ion of	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21	https://ww w.advantech. com/en/sup	O-ADV-EKI 170523/1553

0-1

1-2

3-4 4-5 2-3 Page 647 of 1106

5-6

7-8

6-7

8-9

bounds08-May-20238.8vumer ability, winch can be triggered by authenticated users via a crafted POST request.port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBL17052Product: eki-1524_firmwareAffected Version(s): * Up to (including) 1.21Improper Neutralizat ion of SpecialAdvantech EKI-1524, devices through 1.21https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBLProduct: eki-1524_firmwareAdvantech EKI-1524, devices through 1.21https://ww w.advantech. com/en/sup port/details/ om/en/sup	atch NCIIPC ID	Patch	Description & CVE ID	CVSSv3	Publish Date	Weakness	
Out-of- bounds Write08-May-20238.8Advantech EKI-1524, EKI-1522, EKI-1521 are affected by a Stack-based Buffer Overflow vulnerability, which can be triggered by authenticated users via a crafted POST request. CVE ID : CVE-2023- 2575w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBIL0-ADV 17052Product: ek-t-tstation8.8Advantech EKI-1524, ekritesNttps://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBLImproper Neutralizat ion of Special Elements used in a Command08-May-20238.8Advantech EKI-1524, ekriteshttps://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEB1.0-ADV ordetails/ firmware?id =1-1J9BEB1.	vare?id 9BED3, //ww antech. en/sup details/ vare?id 9BECT, //ww antech. en/sup details/ vare?id	firmware?id =1-1J9BED3, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id	command injection vulnerability in the device name input field, which can be triggered by authenticated users via a crafted POST request. <b>CVE ID : CVE-2023-</b>			Elements used in a Command ('Comman d	
Affected Version(s): * Up to (including) 1.21Improper Neutralizat ion of Special Elements used in aAdvantech EKI-1524, EKI-1522, EKI-1521https://ww w.advantech. com/en/sup port/details/ firmware?id ion of devices through 1.21https://ww w.advantech. com/en/sup port/details/ 17052Special Elements used in a Command08-May-20238.8Advantech EKI-1522, EKI-1521 are affected by an command injection vulnerability in the in the intps://ww0-ADV 0-ADV 17052	antech. en/sup details/ vare?id 9BED3, //ww antech. en/sup details/ 7BECT, //ww antech. en/sup details/ are?id 9BECT, //ww antech. en/sup details/ rare?id	w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id	EKI-1522, EKI-1521 devices through 1.21 are affected by a Stack-based Buffer Overflow vulnerability, which can be triggered by authenticated users via a crafted POST request. <b>CVE ID : CVE-2023-</b>	8.8	08-May-2023	bounds	
Improper Neutralizat ion of Special used in aAdvantech EKI-1524, EKI-1522, EKI-1521https://ww w.advantech. com/en/sup port/details/ firmware?id are affected by an vulnerability in the NTP server inputhttps://ww https://wwAdvantech EKI-1524, w.advantech. om/en/sup port/details/ 17052							
Neutralizat ion of Special Elements used in a Command08-May-2023EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection NTP server inputw.advantech. com/en/sup port/details/ firmware?id 17052							
	antech. en/sup details/ O-ADV-EKI rare?id 170523/1555 9BED3, //ww	w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3, https://ww	EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the NTP server input	8.8	08-May-2023	Neutralizat ion of Special Elements used in a Command	
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-           Page 648 of 1106							

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			triggered by authenticated users via a crafted POST request. CVE ID : CVE-2023- 2573	com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBL	
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the device name input field, which can be triggered by authenticated users via a crafted POST request. <b>CVE ID : CVE-2023- 2574</b>	https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BEBL	O-ADV-EKI 170523/1556
Out-of- bounds Write	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stack-based Buffer Overflow vulnerability, which can be triggered by authenticated users via a crafted POST request. <b>CVE ID : CVE-2023- 2575</b>	https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BED3, https://ww w.advantech. com/en/sup port/details/ firmware?id =1-1J9BECT, https://ww w.advantech.	O-ADV-EKI 170523/1557

0-1

1-2

**2-3** 3-4 4-5 Page **649** of **1106**  5-6

6-7

7-8 8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				com/en/sup port/details/ firmware?id =1-1J9BEBL	
Vendor: aig	ital				
Product: wi	reless-n_repeat	er_mini_r	outer_firmware		
Affected Ver	sion(s): 0.131229	9		1	
Insufficient Session Expiration	02-May-2023	7.5	An issue in the time- based authentication mechanism of Aigital Aigital Wireless-N Repeater Mini_Router v0.131229 allows attackers to bypass login by connecting to the web app after a successful attempt by a legitimate user.	N/A	0-AIG-WIRE- 170523/1558
Vendor: Am	azon		CVE ID : CVE-2023- 30403		
Product: fir					
		excluding)	6.2.9.5		
Use of Insufficient ly Random Values	03-May-2023	8.8	Improper JPAKE implementation allows offline PIN brute-forcing due to the initialization of random values to a known value, which leads to unauthorized authentication to amzn.lightning services. This issue affects:	N/A	O-AMA-FIRE- 170523/1559

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5.		
			Insignia TV with FireOS 7.6.3.3.		
			CVE ID : CVE-2023- 1385		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	The setMediaSource function on the amzn.thin.pl service does not sanitize the "source" parameter allowing for arbitrary javascript code to be run This issue affects:	N/A	0-AMA-FIRE-
			Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS versions prior to 7.6.3.3. CVE ID : CVE-2023- 1384		170523/1560
N/A	03-May-2023	4.3	An Improper Enforcement of Behavioral Workflow vulnerability in the exchangeDeviceServi ces function on the amzn.dmgr service allowed an attacker to register services that are only locally accessible.	N/A	O-AMA-FIRE- 170523/1561
			This issue affects:		

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS versions prior to 7.6.3.3.		
			CVE ID : CVE-2023- 1383		
Affected Ver	sion(s): * Up to (e	excluding)	7.6.3.3		
Use of Insufficient ly Random Values	03-May-2023	8.8	Improper JPAKE implementation allows offline PIN brute-forcing due to the initialization of random values to a known value, which leads to unauthorized authentication to amzn.lightning services. This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS 7.6.3.3. <b>CVE ID : CVE-2023- 1385</b>	N/A	0-AMA-FIRE- 170523/1562
Improper Neutralizat ion of Input During Web Page Generation	03-May-2023	6.1	The setMediaSource function on the amzn.thin.pl service does not sanitize the "source" parameter allowing for arbitrary javascript code to be run	N/A	O-AMA-FIRE- 170523/1563
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b>	6-7 7-8	8 8-9 9-10

Page 652 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
('Cross-site Scripting')			This issue affects:			
			Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5.			
			Insignia TV with FireOS versions prior to 7.6.3.3.			
			CVE ID : CVE-2023- 1384			
N/A	03-May-2023	4.3	An Improper Enforcement of Behavioral Workflow vulnerability in the exchangeDeviceServi ces function on the amzn.dmgr service allowed an attacker to register services that are only locally accessible. This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS versions prior to 7.6.3.3. <b>CVE ID : CVE-2023-</b> <b>1383</b>	N/A	O-AMA-FIRE- 170523/1564	
Vendor: App	ple				L	
Product: ipa						
Affected Ver	sion(s): * Up to (e	excluding)				
N/A	08-May-2023	7.8	The issue was addressed with improved bounds	https://supp ort.apple.co m/en-	O-APP-IPAD- 170523/1565	
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10						
	-		Page <b>653</b> of <b>1106</b>			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checks. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 23536</b>	us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/kb/HT21 3675	
Out-of- bounds Write	08-May-2023	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to cause unexpected system termination or write kernel memory <b>CVE ID : CVE-2023- 27936</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-IPAD- 170523/1566
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5,	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co	O-APP-IPAD- 170523/1567

0-1

1-2

**2-3** 3-4 4-5 Page **654** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023- 23535</b>	m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to read sensitive location information <b>CVE ID : CVE-2023- 23537</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp	O-APP-IPAD- 170523/1568

0-1

1-2

**2-3** 3-4 4-5 Page **655** of **1106**  5-6

6-7

7-8 8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4. An app may be able to disclose kernel memory <b>CVE ID : CVE-2023- 27941</b>	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/kb/HT21 3675	O-APP-IPAD- 170523/1569
Affected Ver	sion(s): * Up to (e	excluding)	16.4		
N/A	08-May-2023	9.8	This was addressed with additional checks by Gatekeeper on files downloaded from an iCloud shared-by-me folder. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. A file from an iCloud shared-by-me folder may be able to bypass Gatekeeper <b>CVE ID : CVE-2023- 23526</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPAD- 170523/1570
N/A	08-May-2023	8.8	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co	O-APP-IPAD- 170523/1571

0-1

1-2

**2-3** 3-4 4-5 Page **656** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to break out of its sandbox CVE ID : CVE-2023- 23532	m/en- us/HT21367 6	
N/A	08-May-2023	7.8	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be able to gain root privileges <b>CVE ID : CVE-2023- 23525</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/kb/HT21 3675	O-APP-IPAD- 170523/1572
Integer Overflow or Wraparoun d	08-May-2023	7.8	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. Parsing a maliciously crafted plist may lead to an unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 27937</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6,	O-APP-IPAD- 170523/1573

0-1

1-2

**2-3** 3-4 4-5 Page **657** of **1106**  5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	6.7	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app with root privileges may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 27933</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-IPAD- 170523/1574
Out-of- bounds Read	08-May-2023	6.5	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in tvOS 16.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted Bluetooth packet may result in disclosure of process memory	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPAD- 170523/1575

0-1

1-2

2-3

3-44-5Page 658 of 1106

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23528		
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. A user may gain access to protected parts of the file system <b>CVE ID : CVE-2023- 23527</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7 6,	0-APP-IPAD- 170523/1576
Out-of- bounds Read	08-May-2023	5.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp	O-APP-IPAD- 170523/1577

0-1

1-2

**2-3** 3-4 4-5 Page **659** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure of process memory CVE ID : CVE-2023- 27929	ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data <b>CVE ID : CVE-2023-</b> <b>27931</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/kb/HT21 3604, https://supp ort.apple.co m/kb/HT21 3603	O-APP-IPAD- 170523/1578
N/A	08-May-2023	5.5	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3,	https://supp ort.apple.co m/en- us/HT21367 4, https://supp	O-APP-IPAD- 170523/1579

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			watchOS 9.4, tvOS 16.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. Processing maliciously crafted web content may bypass Same Origin Policy <b>CVE ID : CVE-2023- 27932</b>	ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data <b>CVE ID : CVE-2023- 27942</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7,	O-APP-IPAD- 170523/1580

0-1

1-2

**2-3** 3-4 4-5 Page **661** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://supp ort.apple.co m/kb/HT21 3675	
N/A	08-May-2023	5.5	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. Files downloaded from the internet may not have the quarantine flag applied <b>CVE ID : CVE-2023- 27943</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPAD- 170523/1581
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	5.3	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to cause a denial-of-service <b>CVE ID : CVE-2023-</b>	https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPAD- 170523/1582
N/A	08-May-2023	3.3	23494 A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. Photos belonging to the Hidden Photos Album could be viewed without authentication	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPAD- 170523/1583

0-1

1-2

**2-3** 3-4 4-5 Page **662** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through Visual Lookup CVE ID : CVE-2023- 23523		
Affected Ver	sion(s): From (in	cluding) 1	6.0 Up to (excluding) 1	6.4	
N/A	08-May-2023	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 23536</b>	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/kb/HT21 3675	O-APP-IPAD- 170523/1584
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023- 23535</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367	O-APP-IPAD- 170523/1585

0-1

1-2

**2-3** 3-4 4-5 Page **663** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to read sensitive location information <b>CVE ID : CVE-2023- 23537</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPAD- 170523/1586
Product: ip	ad_os				·
Affected Ver	sion(s): * Up to (	excluding)	15.7.4		
N/A	08-May-2023	9.8	This issue was addressed with improved state management. This issue is fixed in	https://supp ort.apple.co m/en- us/HT21367 3,	O-APP-IPAD- 170523/1587
CVSS Scoring	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>664</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A remote user may be able to cause unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 28201</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 6	
Out-of- bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 27946</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-IPAD- 170523/1588
Out-of- bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en-	O-APP-IPAD- 170523/1589

0-1

1-2

**2-3** 3-4 4-5 Page **665** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.7.4. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023-</b>	us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	
Use After Free	08-May-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 27969</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	0-APP-IPAD- 170523/1590
N/A	08-May-2023	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367	O-APP-IPAD- 170523/1591

0-1

1-2

**2-3** 3-4 4-5 Page **666** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A shortcut may be able to use sensitive data with certain actions without prompting the user <b>CVE ID : CVE-2023- 27963</b>	0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information <b>CVE ID : CVE-2023- 27954</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en-	O-APP-IPAD- 170523/1592

0-1

1-2

**2-3** 3-4 4-5 Page **667** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT21367 6	
Improper Authentica tion	08-May-2023	6.5	The issue was addressed with improved authentication. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to spoof a VPN server that is configured with EAP- only authentication on a device <b>CVE ID : CVE-2023-</b> <b>28182</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-IPAD- 170523/1593
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp	O-APP-IPAD- 170523/1594

0-1

1-2

**2-3** 3-4 4-5 Page **668** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 27956	ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a maliciously crafted calendar invitation may exfiltrate user information <b>CVE ID : CVE-2023- 27961</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	0-APP-IPAD- 170523/1595
Improper Input Validation	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This	https://supp ort.apple.co m/en- us/HT21367	O-APP-IPAD- 170523/1596

0-1

1-2

**2-3** 3-4 4-5 Page **669** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to disclose kernel memory <b>CVE ID : CVE-2023-</b> <b>28200</b>	5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	
Affected Ver	sion(s): * Up to (e	excluding)	16.4		
N/A	08-May-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 27959</b>	https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPAD- 170523/1597
Out-of- bounds Write	08-May-2023	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 27970</b>	https://supp ort.apple.co m/en- us/HT21367 6	0-APP-IPAD- 170523/1598

0-1

1-2

**2-3** 3-4 4-5 Page **670** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-May-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 28181</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPAD- 170523/1599
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5, iOS 16.4 and iPadOS 16.4. An app may be able to read arbitrary files <b>CVE ID : CVE-2023- 27955</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-IPAD- 170523/1600
N/A	08-May-2023	5.5	A logic issue was addressed with improved validation.	https://supp ort.apple.co m/en-	O-APP-IPAD- 170523/1601

0-1

1-2

2-33-44-5Page 671 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4. An app may be able to bypass Privacy preferences <b>CVE ID : CVE-2023-</b> <b>28178</b>	us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	3.3	The issue was addressed with improved checks. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to unexpectedly create a bookmark on the Home Screen <b>CVE ID : CVE-2023-</b> <b>28194</b>	https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPAD- 170523/1602
Affected Ver	sion(s): From (in	cluding) 1	6.0 Up to (excluding) 1	6.4	
N/A	08-May-2023	9.8	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A remote user may be able to cause unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 28201</b>	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en-	O-APP-IPAD- 170523/1603

0-1

1-2

2-33-44-5Page 672 of 1106

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT21367 6	
Use After Free	08-May-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 27969</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPAD- 170523/1604
N/A	08-May-2023	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A shortcut may be able to use sensitive data with certain actions	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp	O-APP-IPAD- 170523/1605

0-1

1-2

 2-3
 3-4
 4-5

 Page 673 of 1106

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without prompting the user CVE ID : CVE-2023- 27963	ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information <b>CVE ID : CVE-2023- 27954</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	0-APP-IPAD- 170523/1606
Improper Authentica tion	08-May-2023	6.5	The issue was addressed with improved authentication. This	https://supp ort.apple.co m/en- us/HT21367	O-APP-IPAD- 170523/1607

0-1

1-2

**2-3** 3-4 4-5 Page **674** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to spoof a VPN server that is configured with EAP- only authentication on a device <b>CVE ID : CVE-2023- 28182</b>	5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023- 27956</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en-	O-APP-IPAD- 170523/1608

0-1

1-2

2-33-44-5Page 675 of 1106

5-6

6-7

7-8 8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT21367 6	
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a maliciously crafted calendar invitation may exfiltrate user information <b>CVE ID : CVE-2023- 27961</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	0-APP-IPAD- 170523/1609
Product: ip	hone_os			<u> </u>	
Affected Ver	sion(s): * Up to (e	excluding)	15.7.4		
N/A	08-May-2023	9.8	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367	O-APP-IPHO- 170523/1610
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5-6	6-7 7-8	<u> </u>
			Page <b>676</b> of <b>1106</b>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 16.4. A remote user may be able to cause unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023-</b> <b>28201</b>	0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 23536</b>	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/kb/HT21 3675	O-APP-IPHO- 170523/1611
Out-of- bounds Write	08-May-2023	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to cause unexpected system	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en-	O-APP-IPHO- 170523/1612

0-1

1-2

**2-3** 3-4 4-5 Page **677** of **1106**  5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			termination or write kernel memory CVE ID : CVE-2023- 27936	us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	
Out-of- bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 27946</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-IPHO- 170523/1613
Out-of- bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-IPHO- 170523/1614

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 27949		
Use After Free	08-May-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 27969</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPHO- 170523/1615
N/A	08-May-2023	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A shortcut may be able to use sensitive data with certain actions	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp	O-APP-IPHO- 170523/1616

0-1

1-2

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without prompting the user CVE ID : CVE-2023- 27963	ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information <b>CVE ID : CVE-2023- 27954</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	0-APP-IPH0- 170523/1617
Improper Authentica tion	08-May-2023	6.5	The issue was addressed with improved authentication. This	https://supp ort.apple.co m/en- us/HT21367	O-APP-IPHO- 170523/1618

0-1

1-2

**2-3** 3-4 4-5 Page **680** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to spoof a VPN server that is configured with EAP- only authentication on a device <b>CVE ID : CVE-2023- 28182</b>	5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023- 23535</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en-	O-APP-IPHO- 170523/1619

0-1

1-2

2-33-44-5Page 681 of 1106

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to read sensitive location information <b>CVE ID : CVE-2023- 23537</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPHO- 170523/1620
N/A	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4. An app may be able to disclose kernel memory	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp	O-APP-IPHO- 170523/1621

0-1

1-2

**2-3** 3-4 4-5 Page **682** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 27941	ort.apple.co m/kb/HT21 3675	
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023- 27956</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPHO- 170523/1622
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0,	O-APP-IPHO- 170523/1623

0-1

1-2

**2-3** 3-4 4-5 Page **683** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted calendar invitation may exfiltrate user information CVE ID : CVE-2023- 27961	https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
Improper Input Validation	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to disclose kernel memory <b>CVE ID : CVE-2023-</b> <b>28200</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-IPHO- 170523/1624
Affected Ver	sion(s): * Up to (e	excluding)	16.4	<u> </u>	l
N/A	08-May-2023	9.8	This was addressed with additional checks by Gatekeeper on files downloaded from an iCloud shared-by-me folder. This issue is	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co	O-APP-IPHO- 170523/1625

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. A file from an iCloud shared-by-me folder may be able to bypass Gatekeeper	m/en- us/HT21367 6	
			CVE ID : CVE-2023- 23526		
N/A	08-May-2023	8.8	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be able to break out of its sandbox <b>CVE ID : CVE-2023- 23532</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6	0-APP-IPHO- 170523/1626
N/A	08-May-2023	7.8	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be able to gain root privileges <b>CVE ID : CVE-2023- 23525</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/kb/HT21 3675	O-APP-IPHO- 170523/1627
Integer Overflow or Wraparoun d	08-May-2023	7.8	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en-	O-APP-IPHO- 170523/1628

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. Parsing a maliciously crafted plist may lead to an unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023-</b> <b>27937</b>	us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 27959</b>	https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPHO- 170523/1629
Out-of- bounds Write	08-May-2023	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary	https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPHO- 170523/1630

0-1

1-2

**2-3** 3-4 4-5 Page **686** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with kernel privileges CVE ID : CVE-2023- 27970		
N/A	08-May-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 28181</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPHO- 170523/1631
N/A	08-May-2023	6.7	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app with root privileges may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 27933</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367	O-APP-IPHO- 170523/1632

0-1

1-2

**2-3** 3-4 4-5 Page **687** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				6, https://supp ort.apple.co m/en- us/HT21367 7	
Out-of- bounds Read	08-May-2023	6.5	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in tvOS 16.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted Bluetooth packet may result in disclosure of process memory <b>CVE ID : CVE-2023- 23528</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 6	0-APP-IPHO- 170523/1633
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. A user may gain access to protected parts of the file system <b>CVE ID : CVE-2023- 23527</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co	O-APP-IPHO- 170523/1634

0-1

1-2

**2-3** 3-4 4-5 Page **688** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
Out-of- bounds Read	08-May-2023	5.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023- 27929</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPHO- 170523/1635
N/A	08-May-2023	5.5	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data <b>CVE ID : CVE-2023- 27931</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8,	O-APP-IPHO- 170523/1636

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/kb/HT21 3604, https://supp ort.apple.co m/kb/HT21 3603	
N/A	08-May-2023	5.5	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. Processing maliciously crafted web content may bypass Same Origin Policy <b>CVE ID : CVE-2023- 27932</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	0-APP-IPHO- 170523/1637
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3,	https://supp ort.apple.co m/en- us/HT21367 4,	O-APP-IPHO- 170523/1638

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data <b>CVE ID : CVE-2023- 27942</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7, https://supp ort.apple.co m/kb/HT21 3675	
N/A	08-May-2023	5.5	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. Files downloaded from the internet may not have the quarantine flag applied <b>CVE ID : CVE-2023- 27943</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPHO- 170523/1639
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey	https://supp ort.apple.co m/en- us/HT21367 5, https://supp	O-APP-IPHO- 170523/1640

0-1

1-2

2-33-44-5Page 691 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.6.4, macOS Big Sur 11.7.5, iOS 16.4 and iPadOS 16.4. An app may be able to read arbitrary files <b>CVE ID : CVE-2023-</b> <b>27955</b>	ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	5.5	A logic issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4. An app may be able to bypass Privacy preferences <b>CVE ID : CVE-2023- 28178</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-IPHO- 170523/1641
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	5.3	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to cause a denial-of-service <b>CVE ID : CVE-2023- 23494</b>	https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPHO- 170523/1642

0-1

1-2

2-33-44-5Page 692 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-May-2023	3.3	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. Photos belonging to the Hidden Photos Album could be viewed without authentication through Visual Lookup <b>CVE ID : CVE-2023- 23523</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPHO- 170523/1643
N/A	08-May-2023	3.3	The issue was addressed with improved checks. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to unexpectedly create a bookmark on the Home Screen <b>CVE ID : CVE-2023-</b> <b>28194</b>	https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPHO- 170523/1644
Affected Ver	sion(s): From (in	cluding) 1	6.0 Up to (excluding) 1	6.4	
N/A	08-May-2023	9.8	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A remote user may be able to cause unexpected app	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en-	O-APP-IPHO- 170523/1645

0-1

1-2

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			termination or arbitrary code execution CVE ID : CVE-2023- 28201	us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 6	
Use After Free	08-May-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 27969</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	0-APP-IPHO- 170523/1646
N/A	08-May-2023	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp	O-APP-IPHO- 170523/1647

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.4. A shortcut may be able to use sensitive data with certain actions without prompting the user <b>CVE ID : CVE-2023-</b> <b>27963</b>	ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information <b>CVE ID : CVE-2023- 27954</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en-	0-APP-IPHO- 170523/1648

0-1

1-2

**2-3** 3-4 4-5 Page **695** of **1106**  5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT21367 6	
Improper Authentica tion	08-May-2023	6.5	The issue was addressed with improved authentication. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to spoof a VPN server that is configured with EAP- only authentication on a device <b>CVE ID : CVE-2023-</b> <b>28182</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-IPHO- 170523/1649
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp	O-APP-IPHO- 170523/1650

0-1

1-2

**2-3** 3-4 4-5 Page **696** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 23535	ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to read sensitive location information <b>CVE ID : CVE-2023- 23537</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-IPHO- 170523/1651
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue	https://supp ort.apple.co m/en- us/HT21367	O-APP-IPHO- 170523/1652

0-1

1-2

**2-3** 3-4 4-5 Page **697** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023- 27956</b>	4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a maliciously crafted calendar invitation may exfiltrate user information <b>CVE ID : CVE-2023- 27961</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en-	O-APP-IPHO- 170523/1653

0-1

1-2

**2-3** 3-4 4-5 Page **698** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
Product: ma					
Affected Ver	sion(s): -			Γ	
Improper Enforceme nt of Message Integrity During Transmissi on in a Communic ation Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 22372</b>	https://my.f 5.com/mana ge/s/article/ K000132522	O-APP-MACO- 170523/1654
Improper Certificate Validation	03-May-2023	5.9	An improper certificate validation vulnerabil ity exists in the BIG- IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000132539	O-APP-MACO- 170523/1655

0-1

1-2

**2-3** 3-4 4-5 Page **699** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24461		
Affected Ver	sion(s): * Up to (	excluding)	10.4.8		
Out-of- bounds Read	08-May-2023	7.8	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in GarageBand for macOS 10.4.8. Parsing a maliciously crafted MIDI file may lead to an unexpected application termination or arbitrary code execution <b>CVE ID : CVE-2023- 27938</b>	https://supp ort.apple.co m/en- us/HT21365 0	O-APP-MACO- 170523/1656
Affected Ver	sion(s): * Up to (	excluding)	11.7.5		
N/A	08-May-2023	8.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 27935</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1657
N/A	08-May-2023	8.6	This issue was addressed with a new entitlement. This issue is fixed in	https://supp ort.apple.co m/en- us/HT21367	O-APP-MACO- 170523/1658

0-1

1-2

**2-3** 3-4 4-5 Page **700** of **1106**  8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to break out of its sandbox <b>CVE ID : CVE-2023-</b> <b>27944</b>	5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	
Out-of- bounds Write	08-May-2023	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to cause unexpected system termination or write kernel memory <b>CVE ID : CVE-2023- 27936</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1659
Integer Overflow or Wraparoun d	08-May-2023	7.8	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. Parsing a maliciously	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co	O-APP-MACO- 170523/1660

0-1

1-2

2-33-44-5Page 701 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted plist may lead to an unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023-</b> <b>27937</b>	m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. A user may gain access to protected parts of the file system <b>CVE ID : CVE-2023- 23527</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp	0-APP-MACO- 170523/1661

0-1

1-2

2-33-44-5Page 702 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023- 23534</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0	O-APP-MACO- 170523/1662
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023- 23535</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp	O-APP-MACO- 170523/1663

0-1

1-2

2-33-44-5Page 703 of 1106

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to read sensitive location information <b>CVE ID : CVE-2023- 23537</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-MACO- 170523/1664
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An archive may be able to bypass Gatekeeper <b>CVE ID : CVE-2023- 27951</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en-	O-APP-MACO- 170523/1665

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT21367 7	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3. An app may be able to view sensitive information <b>CVE ID : CVE-2023- 28189</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/kb/HT21 3675	O-APP-MACO- 170523/1666
Affected Ver	sion(s): * Up to (e	excluding)	12.6.4	1	
N/A	08-May-2023	6.7	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app with root privileges may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 27933</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1667
N/A	08-May-2023	5.5	A logic issue was addressed with improved checks. This issue is fixed in	https://supp ort.apple.co m/en- us/HT21367	O-APP-MACO- 170523/1668

0-1

1-2

**2-3** 3-4 4-5 Page **705** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Ventura 13.3, macOS Monterey 12.6.4. An app may be able to modify protected parts of the file system	0, https://supp ort.apple.co m/en- us/HT21367 7	
			CVE ID : CVE-2023- 23533		
N/A	08-May-2023	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4. An app may be able to modify protected parts of the file system <b>CVE ID : CVE-2023-</b> <b>23538</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1669
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data <b>CVE ID : CVE-2023- 27942</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en-	O-APP-MACO- 170523/1670

0-1

1-2

**2-3** 3-4 4-5 Page **706** of **1106**  5-6

6-7

8-9

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT21367 7, https://supp ort.apple.co m/kb/HT21 3675	
Affected Ver	sion(s): * Up to (e	excluding)	13.3		-
N/A	08-May-2023	9.8	This was addressed with additional checks by Gatekeeper on files downloaded from an iCloud shared-by-me folder. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. A file from an iCloud shared-by-me folder may be able to bypass Gatekeeper <b>CVE ID : CVE-2023-</b> 23526	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-MACO- 170523/1671
N/A	08-May-2023	8.8	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be able to break out of its sandbox <b>CVE ID : CVE-2023-</b> <b>23532</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-MACO- 170523/1672
Improper Initializatio n	08-May-2023	8.8	A memory initialization issue was addressed. This issue is fixed in macOS Ventura 13.3. A remote user may be able to cause unexpected app	https://supp ort.apple.co m/en- us/HT21367 0	O-APP-MACO- 170523/1673

0-1

1-2

2-3 3-4 4-5 Page **707** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			termination or arbitrary code execution		
			CVE ID : CVE-2023- 27934		
N/A	08-May-2023	7.8	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be able to gain root privileges <b>CVE ID : CVE-2023- 23525</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/kb/HT21 3675	O-APP-MACO- 170523/1674
N/A	08-May-2023	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 23536</b>	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/kb/HT21 3675	O-APP-MACO- 170523/1675
N/A	08-May-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS	https://supp ort.apple.co m/en- us/HT21367 4,	O-APP-MACO- 170523/1676

0-1

1-2

**2-3** 3-4 4-5 Page **708** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 28181</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	6.5	A denial-of-service issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. A user in a privileged network position may be able to cause a denial-of-service <b>CVE ID : CVE-2023- 28180</b>	https://supp ort.apple.co m/en- us/HT21367 0	O-APP-MACO- 170523/1677
Out-of- bounds Read	08-May-2023	5.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023- 27929</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp	O-APP-MACO- 170523/1678

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data <b>CVE ID : CVE-2023- 27931</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/kb/HT21 3604, https://supp ort.apple.co m/kb/HT21 3603	O-APP-MACO- 170523/1679
N/A	08-May-2023	5.5	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. Processing maliciously crafted	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp	O-APP-MACO- 170523/1680

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web content may bypass Same Origin Policy <b>CVE ID : CVE-2023-</b> <b>27932</b>	ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4. An app may be able to disclose kernel memory <b>CVE ID : CVE-2023- 27941</b>	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/kb/HT21 3675	O-APP-MACO- 170523/1681
N/A	08-May-2023	5.5	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. Files downloaded from the internet may not have the quarantine flag applied <b>CVE ID : CVE-2023- 27943</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-MACO- 170523/1682

0-1

1-2

2-33-44-5Page 711 of 1106

6-7 7-8

5-6

N/A	08-May-2023		A privacy issue was addressed by moving sensitive data to a more secure		
		5.5	location. This issue is fixed in macOS Ventura 13.3. An app may be able to access user-sensitive data <b>CVE ID : CVE-2023-</b> <b>28190</b>	https://supp ort.apple.co m/en- us/HT21367 0	O-APP-MACO- 170523/1683
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	08-May-2023	4.7	A race condition was addressed with improved locking. This issue is fixed in macOS Ventura 13.3. An app may bypass Gatekeeper checks <b>CVE ID : CVE-2023- 27952</b>	https://supp ort.apple.co m/en- us/HT21367 0	O-APP-MACO- 170523/1684
N/A	08-May-2023	3.3	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. Photos belonging to the Hidden Photos Album could be viewed without authentication through Visual Lookup <b>CVE ID : CVE-2023- 23523</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-MACO- 170523/1685

0-1

1-2

2-3 3-4 4-5 Page 712 of 1106 5-6

6-7

7-8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	08-May-2023	9.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory <b>CVE ID : CVE-2023- 27953</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1686
N/A	08-May-2023	9.1	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory <b>CVE ID : CVE-2023- 27958</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1687
Out-of- bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. Processing a	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp	O-APP-MACO- 170523/1688

0-1

1-2

2-33-44-5Page 713 of 1106

6-7

5-6

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted file may lead to unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 27946</b>	ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	
Improper Authentica tion	08-May-2023	6.5	The issue was addressed with improved authentication. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to spoof a VPN server that is configured with EAP- only authentication on a device <b>CVE ID : CVE-2023- 28182</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1689
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5, iOS 16.4 and iPadOS 16.4. An	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367	O-APP-MACO- 170523/1690

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			app may be able to read arbitrary files CVE ID : CVE-2023- 27955	0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a maliciously crafted calendar invitation may exfiltrate user information <b>CVE ID : CVE-2023- 27961</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	0-APP-MACO- 170523/1691
N/A	08-May-2023	5.5	A logic issue was addressed with	https://supp ort.apple.co	O-APP-MACO- 170523/1692

0-1

1-2

2-33-44-5Page 715 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to modify protected parts of the file system <b>CVE ID : CVE-2023- 27962</b>	m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	
Incorrect Default Permission s	08-May-2023	5.5	A permissions issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to read sensitive location information <b>CVE ID : CVE-2023- 28192</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1693
Improper Input Validation	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to disclose kernel memory <b>CVE ID : CVE-2023- 28200</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0,	O-APP-MACO- 170523/1694

0-1

1-2

2-33-44-5Page 716 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://supp ort.apple.co m/en- us/HT21367 7	
Affected Ver	sion(s): From (in	cluding) 1	2.0 Up to (excluding) 12	2.6.4	
Out-of- bounds Write	08-May-2023	9.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Wonterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory <b>CVE ID : CVE-2023- 27953</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1695
N/A	08-May-2023	9.1	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Wonterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory <b>CVE ID : CVE-2023- 27958</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1696
N/A	08-May-2023	8.8	The issue was addressed with improved bounds checks. This issue is	https://supp ort.apple.co m/en- us/HT21367	O-APP-MACO- 170523/1697

0-1

1-2

2-33-44-5Page 717 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 27935</b>	5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	8.6	This issue was addressed with a new entitlement. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to break out of its sandbox <b>CVE ID : CVE-2023-</b> <b>27944</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1698
Out-of- bounds Write	08-May-2023	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to cause unexpected system termination or write kernel memory	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp	O-APP-MACO- 170523/1699

0-1

1-2

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 27936	ort.apple.co m/en- us/HT21367 7	
Integer Overflow or Wraparoun d	08-May-2023	7.8	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. Parsing a maliciously crafted plist may lead to an unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 27937</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	0-APP-MAC0- 170523/1700
Out-of- bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4,	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367	O-APP-MACO- 170523/1701

0-1

1-2

2-33-44-5Page 719 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Big Sur 11.7.5. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 27946</b>	3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	
Out-of- bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 27949</b>	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1702
N/A	08-May-2023	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A shortcut may be able to use sensitive data with certain actions	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8,	O-APP-MACO- 170523/1703

0-1

1-2

2-33-44-5Page 720 of 1106

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without prompting the user <b>CVE ID : CVE-2023-</b> <b>27963</b>	https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
Improper Authentica tion	08-May-2023	6.5	The issue was addressed with improved authentication. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to spoof a VPN server that is configured with EAP- only authentication on a device <b>CVE ID : CVE-2023- 28182</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1704
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4,	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en-	O-APP-MACO- 170523/1705

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. A user may gain access to protected parts of the file system <b>CVE ID : CVE-2023-</b> 23527	us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An archive may be able to bypass Gatekeeper <b>CVE ID : CVE-2023-</b> <b>27951</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1706
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey	https://supp ort.apple.co m/en- us/HT21367 5, https://supp	O-APP-MACO- 170523/1707

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.6.4, macOS Big Sur 11.7.5, iOS 16.4 and iPadOS 16.4. An app may be able to read arbitrary files <b>CVE ID : CVE-2023-</b> <b>27955</b>	ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a maliciously crafted calendar invitation may exfiltrate user information <b>CVE ID : CVE-2023- 27961</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en-	O-APP-MACO- 170523/1708

0-1

1-2

2-33-44-5Page 723 of 1106

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT21367 7	
N/A	08-May-2023	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to modify protected parts of the file system <b>CVE ID : CVE-2023-</b> <b>27962</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1709
N/A	08-May-2023	5.5	A logic issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4. An app may be able to bypass Privacy preferences <b>CVE ID : CVE-2023- 28178</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1710
Incorrect Default Permission s	08-May-2023	5.5	A permissions issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to read sensitive location information	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp	O-APP-MACO- 170523/1711

0-1

1-2

3-4 4-5 2-3 Page 724 of 1106

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 28192	ort.apple.co m/en- us/HT21367 7	
Improper Input Validation	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to disclose kernel memory <b>CVE ID : CVE-2023-</b> <b>28200</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1712
Affected Ver	sion(s): From (in	cluding) 1	3.0 Up to (excluding) 1	3.3	
N/A	08-May-2023	9.8	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A remote user may be able to cause unexpected app termination or arbitrary code execution	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en-	O-APP-MACO- 170523/1713

0-1

1-2

2-33-44-5Page 725 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 28201	us/HT21367 6	
Out-of- bounds Write	08-May-2023	9.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory <b>CVE ID : CVE-2023- 27953</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1714
N/A	08-May-2023	9.1	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory <b>CVE ID : CVE-2023- 27958</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1715
N/A	08-May-2023	8.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en-	O-APP-MACO- 170523/1716

0-1

1-2

**2-3** 3-4 4-5 Page **726** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11.7.5. A remote user may be able to cause unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023-</b> <b>27935</b>	us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	8.6	This issue was addressed with a new entitlement. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to break out of its sandbox <b>CVE ID : CVE-2023- 27944</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1717
Out-of- bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 27946</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1718

0-1

1-2

2-33-44-5Page 727 of 1106

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 27949</b>	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1719
Out-of- bounds Write	08-May-2023	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to cause unexpected system termination or write kernel memory <b>CVE ID : CVE-2023- 27936</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1720
Integer Overflow or Wraparoun d	08-May-2023	7.8	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS	https://supp ort.apple.co m/en- us/HT21367 4, https://supp	O-APP-MACO- 170523/1721

0-1

1-2

**2-3** 3-4 4-5 Page **728** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. Parsing a maliciously crafted plist may lead to an unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 27937</b>	ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	7.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 27957</b>	https://supp ort.apple.co m/en- us/HT21367 0	O-APP-MACO- 170523/1722
Out-of- bounds Write	08-May-2023	7.8	A memory corruption issue was addressed with improved state	https://supp ort.apple.co m/en- us/HT21367	O-APP-MACO- 170523/1723

0-1

1-2

**2-3** 3-4 4-5 Page **729** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management. This issue is fixed in macOS Ventura 13.3, Studio Display Firmware Update 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023-</b> <b>27965</b>	2, https://supp ort.apple.co m/en- us/HT21367 0	
Use After Free	08-May-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 27969</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-MACO- 170523/1724
N/A	08-May-2023	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co	O-APP-MACO- 170523/1725

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A shortcut may be able to use sensitive data with certain actions without prompting the user <b>CVE ID : CVE-2023- 27963</b>	m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	7.1	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. An app may be able to cause unexpected system termination or write kernel memory <b>CVE ID : CVE-2023- 27968</b>	https://supp ort.apple.co m/en- us/HT21367 0	O-APP-MACO- 170523/1726
N/A	08-May-2023	6.7	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app with root privileges may be able to	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co	O-APP-MACO- 170523/1727

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code with kernel privileges CVE ID : CVE-2023- 27933	m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information <b>CVE ID : CVE-2023- 27954</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	0-APP-MAC0- 170523/1728

0-1

1-2

2-33-44-5Page 732 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentica tion	08-May-2023	6.5	The issue was addressed with improved authentication. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to spoof a VPN server that is configured with EAP- only authentication on a device <b>CVE ID : CVE-2023-</b> <b>28182</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1729
N/A	08-May-2023	6.3	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3. An app may be able to break out of its sandbox <b>CVE ID : CVE-2023- 27966</b>	https://supp ort.apple.co m/en- us/HT21367 0	O-APP-MACO- 170523/1730
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en-	O-APP-MACO- 170523/1731

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023-</b> <b>27956</b>	us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4. An app may be able to modify protected parts of the file system <b>CVE ID : CVE-2023-</b> <b>23533</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1732
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023-</b> <b>23534</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0	O-APP-MACO- 170523/1733

0-1

1-2

**2-3** 3-4 4-5 Page **734** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a maliciously crafted calendar invitation may exfiltrate user information <b>CVE ID : CVE-2023- 27961</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1734
N/A	08-May-2023	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to modify protected parts of the file system	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en-	O-APP-MACO- 170523/1735

0-1

1-2

2-33-44-5Page 735 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 27962	us/HT21367 7	
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023- 23535</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	0-APP-MAC0- 170523/1736
N/A	08-May-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp	O-APP-MACO- 170523/1737

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.4 and iPadOS 16.4. An app may be able to read sensitive location information <b>CVE ID : CVE-2023-</b> <b>23537</b>	ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4. An app may be able to modify protected parts of the file system <b>CVE ID : CVE-2023-</b> <b>23538</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	0-APP-MACO- 170523/1738
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data <b>CVE ID : CVE-2023- 27942</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co	O-APP-MACO- 170523/1739

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7, https://supp ort.apple.co m/kb/HT21 3675	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An archive may be able to bypass Gatekeeper <b>CVE ID : CVE-2023- 27951</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1740
N/A	08-May-2023	5.5	A logic issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4. An app may be able to bypass Privacy preferences <b>CVE ID : CVE-2023-</b> <b>28178</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1741

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. A user may gain access to protected parts of the file system <b>CVE ID : CVE-2023- 23527</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1742
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3. An app may be able to view sensitive information <b>CVE ID : CVE-2023- 28189</b>	https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/kb/HT21 3675	O-APP-MACO- 170523/1743
Incorrect Default	08-May-2023	5.5	A permissions issue was addressed with improved validation.	https://supp ort.apple.co m/en-	O-APP-MACO- 170523/1744

0-1

1-2

**2-3** 3-4 4-5 Page **739** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permission s			This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to read sensitive location information <b>CVE ID : CVE-2023- 28192</b>	us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	
Improper Input Validation	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to disclose kernel memory <b>CVE ID : CVE-2023-</b> <b>28200</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 7	O-APP-MACO- 170523/1745
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5, iOS 16.4 and iPadOS 16.4. An app may be able to read arbitrary files	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp	O-APP-MACO- 170523/1746

0-1

1-2

3-4 4-5 2-3 Page 740 of 1106

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 27955	ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
Product: ma	ac_os_x				
Affected Ver	sion(s): From (in	cluding) 1	0.0 Up to (excluding) 10	).4.8	
N/A	08-May-2023	7.8	This issue was addressed by removing the vulnerable code. This issue is fixed in GarageBand for macOS 10.4.8. An app may be able to gain elevated privileges during the installation of GarageBand <b>CVE ID : CVE-2023- 27960</b>	https://supp ort.apple.co m/en- us/HT21365 0	O-APP-MAC 170523/1747
Product: sa	fari			L	
Affected Ver	sion(s): * Up to (e	excluding)	16.4		
N/A	08-May-2023	5.5	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. Processing maliciously crafted web content may bypass Same Origin Policy	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1,	O-APP-SAFA- 170523/1748
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
CV35 Sconing .		- 2 - 3	J + J - J-0	, , , , , , , , , , , , , , , , , , , ,	

Page 741 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID : CVE-2023- 27932	https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6		
	ıdio_display_firi					
Affected Ver	sion(s): * Up to (e	excluding)	16.4			
Out-of- bounds Write	08-May-2023	7.8	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, Studio Display Firmware Update 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 27965</b>	https://supp ort.apple.co m/en- us/HT21367 2, https://supp ort.apple.co m/en- us/HT21367 0	0-APP-STUD- 170523/1749	
Product: tvo	DS					
Affected Ver	sion(s): * Up to (e	excluding)	16.4			
Integer Overflow or Wraparoun d	08-May-2023	7.8	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. Parsing a maliciously crafted plist may	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en-	O-APP-TVOS- 170523/1750	
				· ·		
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10           Page 742 of 1106						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to an unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023-</b> <b>27937</b>	us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
Use After Free	08-May-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 27969</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-TVOS- 170523/1751

0-1

1-2

2-3 3-4 4-5 Page **743** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-May-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 28181</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-TVOS- 170523/1752
N/A	08-May-2023	6.7	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Wonterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app with root privileges may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 27933</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en-	0-APP-TVOS- 170523/1753

0-1

1-2

**2-3** 3-4 4-5 Page **744** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT21367 7	
Out-of- bounds Read	08-May-2023	6.5	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in tvOS 16.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted Bluetooth packet may result in disclosure of process memory	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-TVOS- 170523/1754
			CVE ID : CVE-2023- 23528		
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information <b>CVE ID : CVE-2023- 27954</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 8, https://supp	0-APP-TVOS- 170523/1755

0-1

1-2

2-3 3-4 4-5 Page **745** of **1106**  5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. A user may gain access to protected parts of the file system <b>CVE ID : CVE-2023-</b> <b>23527</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	0-APP-TVOS- 170523/1756
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367	O-APP-TVOS- 170523/1757

0-1

1-2

2-3 3-4 4-5 Page **746** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023-</b> <b>23535</b>	5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
Out-of- bounds Read	08-May-2023	5.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023- 27929</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-TVOS- 170523/1758
N/A	08-May-2023	5.5	This issue was addressed by	https://supp ort.apple.co	O-APP-TVOS- 170523/1759

0-1

1-2

2-3 3-4 4-5 Page **747** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removing the vulnerable code. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data <b>CVE ID : CVE-2023-</b> 27931	m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/kb/HT21 3604, https://supp ort.apple.co m/kb/HT21 3603	
N/A	08-May-2023	5.5	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. Processing maliciously crafted web content may bypass Same Origin Policy <b>CVE ID : CVE-2023- 27932</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en-	O-APP-TVOS- 170523/1760

0-1

1-2

**2-3** 3-4 4-5 Page **748** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data <b>CVE ID : CVE-2023- 27942</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7, https://supp ort.apple.co m/en- us/HT21367 7, https://supp ort.apple.co m/en- us/HT21367 5	0-APP-TVOS- 170523/1761
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co	O-APP-TVOS- 170523/1762

0-1

1-2

2-3 3-4 4-5 Page **749** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023- 27956</b>	m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
Product: wa	itchos			I	
Affected Ver	sion(s): * Up to (e	excluding)	9.4		
Integer Overflow or Wraparoun d	08-May-2023	7.8	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. Parsing a maliciously crafted plist may lead to an unexpected app termination or arbitrary code execution <b>CVE ID : CVE-2023- 27937</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en-	O-APP-WATC- 170523/1763

0-1

1-2

**2-3** 3-4 4-5 Page **750** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
Use After Free	08-May-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges <b>CVE ID : CVE-2023- 27969</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-WATC- 170523/1764
N/A	08-May-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp	0-APP-WATC- 170523/1765

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with kernel privileges CVE ID : CVE-2023- 28181	ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A shortcut may be able to use sensitive data with certain actions without prompting the user <b>CVE ID : CVE-2023- 27963</b>	https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	0-APP-WATC- 170523/1766
N/A	08-May-2023	6.7	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367	O-APP-WATC- 170523/1767

0-1

1-2

2-33-44-5Page 752 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 16.4. An app with root privileges may be able to execute arbitrary code with kernel privileges CVE ID : CVE-2023- 27933	0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information <b>CVE ID : CVE-2023- 27954</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en-	0-APP-WATC- 170523/1768

0-1

1-2

2-33-44-5Page 753 of 1106

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT21367 6	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. A user may gain access to protected parts of the file system <b>CVE ID : CVE-2023- 23527</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	0-APP-WATC- 170523/1769
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 5, https://supp	O-APP-WATC- 170523/1770

0-1

1-2

**2-3** 3-4 4-5 Page **754** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023-</b> 23535	ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to read sensitive location information <b>CVE ID : CVE-2023- 23537</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en-	O-APP-WATC- 170523/1771

0-1

1-2

2-33-44-5Page 755 of 1106

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT21367 6	
Out-of- bounds Read	08-May-2023	5.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023- 27929</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-WATC- 170523/1772
N/A	08-May-2023	5.5	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data <b>CVE ID : CVE-2023-</b> <b>27931</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp	O-APP-WATC- 170523/1773

0-1

1-2

**2-3** 3-4 4-5 Page **756** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.co m/kb/HT21 3604, https://supp ort.apple.co m/kb/HT21 3603	
N/A	08-May-2023	5.5	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. Processing maliciously crafted web content may bypass Same Origin Policy <b>CVE ID : CVE-2023- 27932</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-WATC- 170523/1774
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app may be able to	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp	O-APP-WATC- 170523/1775

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access user-sensitive data CVE ID : CVE-2023- 27942	ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7, https://supp ort.apple.co m/kb/HT21 3675	
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory <b>CVE ID : CVE-2023- 27956</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	O-APP-WATC- 170523/1776

0-1

1-2

**2-3** 3-4 4-5 Page **758** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a maliciously crafted calendar invitation may exfiltrate user information <b>CVE ID : CVE-2023- 27961</b>	https://supp ort.apple.co m/en- us/HT21367 5, https://supp ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6, https://supp ort.apple.co m/en- us/HT21367 7	0-APP-WATC- 170523/1777
Vendor: Aru					
Product: aru		1 1			
Affected Vers	sion(s): From (in	cluding) 1	0.3.0.0 Up to (including	g) 10.3.1.0	
Improper Neutralizat ion of Special Elements used in a Command ('Comman	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-ARU-ARUB- 170523/1778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b>		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	22788 Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. CVE ID : CVE-2023- 22789	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-ARU-ARUB- 170523/1779
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-ARU-ARUB- 170523/1780

0-1

1-2

**2-3** 3-4 4-5 Page **760** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands as a privileged user on the underlying operating system.		
			CVE ID : CVE-2023- 22790		
N/A	08-May-2023	7.5	An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point. <b>CVE ID : CVE-2023- 22787</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-ARU-ARUB- 170523/1781
N/A	08-May-2023	4.8	A vulnerability exists in Aruba InstantOS and ArubaOS 10 where an edge- case combination of network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-ARU-ARUB- 170523/1782

0-1

1-2

2-33-44-5Page 761 of 1106

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially sensitive		
			information can		
			occur are complex		
			and depend on		
			factors that are		
			beyond the control of		
			the attacker.		
			CVE ID : CVE-2023-		
			22791		
Vendor: Asu					
	ac51u_firmwar				
Affected Vers	sion(s): * Up to (i	ncluding)	3.0.0.4.380.8591		Г
			A Cross-site scripting		
			(XSS) vulnerability in		
			the System		
			Log/General Log		
			page of the		
Improper			administrator web		
Neutralizat			UI in ASUS RT-		
ion of			AC51U wireless		
Input			router firmware		
During	02-May-2023	5.2	version up to and including	N/A	O-ASU-RT-A-
Web Page	5		3.0.0.4.380.8591	,	170523/1783
Generation			allows remote		
('Cross-site			attackers to inject		
Scripting')			arbitrary web script		
			or HTML via a		
			malicious network		
			request.		
			•		
			CVE ID : CVE-2023- 29772		
Vendor: Axi	S				
Product: axi	is_os				
Affected Vers	sion(s): From (in	cluding) 1	1.0.89 Up to (excluding	) 11.4.52	
M: .			AXIS OS 11.0.X -	https://ww	
Missing			11.3.x use a static	w.axis.com/	O AVI AVIO
Encryption	08-May-2023	5.3	RSA key in legacy	dam/public/	0-AXI-AXIS-
of Sensitive	-		LUA-components to	07/0a/20/cv	170523/1784
Data			protect Axis-specific	e-2023-	
			source code. The	21404-en-	
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 <b>762</b> of <b>1106</b>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
	static RSA key is not used in any other secure communication nor can it be used to compromise the device or any customer data. CVE ID : CVE-2023- 21404		US- 398426.pdf		
Vendor: Cis			21404		
	a112_firmware				
	rsion(s): 1.4.1				
Missing Authentica tion for Critical Function	04-May-2023	9.8	A vulnerability in the web-based management interface of Cisco SPA112 2-Port Phone Adapters could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to a missing authentication process within the firmware upgrade function. An attacker could exploit this vulnerability by upgrading an affected device to a crafted version of firmware. A successful exploit could allow the attacker to execute arbitrary code on the affected device with	https://sec.c loudapps.cis co.com/secu rity/center/ content/Cisc oSecurityAd visory/cisco- sa-spa- unauth- upgrade- UqhyTWW	0-CIS-SPA1- 170523/1785

0-1

1-2

2-33-44-5Page 763 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			full privileges. Cisco has not released firmware updates to address this vulnerability.		
			CVE ID : CVE-2023- 20126		
Vendor: cor	ntiki-ng				
Product: co	ntiki-ng				
Affected Ver	sion(s): * Up to (i	ncluding)	4.8		
NULL Pointer Dereferenc e	08-May-2023	9.8	The Contiki-NG operating system versions 4.8 and prior can be triggered to dereference a NULL pointer in the message handling code for IPv6 router solicitiations. Contiki-NG contains an implementation of IPv6 Neighbor Discovery (ND) in the module `os/net/ipv6/uip- nd6.c`. The ND protocol includes a message type called Router Solicitation (RS), which is used to locate routers and update their address information via the SLLAO (Source Link- Layer Address Option). If the indicated source address changes, a given neighbor entry is set to the STALE state.	https://githu b.com/conti ki- ng/contiki- ng/security/ advisories/G HSA-x29r- 5qjg-75mq	0-CON-CONT- 170523/1786

0-1

1-2

**2-3** 3-4 4-5 Page **764** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The message handler does not check for RS messages with an SLLAO that indicates a link-layer address change that a neighbor entry can actually be created for the indicated address. The resulting pointer is used without a check, leading to the dereference of a NULL pointer of type `uip_ds6_nbr_t`.		
			The problem has been patched in the 'develop' branch of Contiki-NG, and will be included in the upcoming 4.9 release. As a workaround, users can apply Contiki-NG pull request #2271 to patch the problem directly.		
			CVE ID : CVE-2023- 31129		
Vendor: Del	bian				
Product: de					
Affected Ver	sion(s): 10.0				
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in	https://supp ort.apple.co m/en- us/HT21367 4,	O-DEB-DEBI- 170523/1787
			macOS Ventura 13.3,	https://supp	

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
			watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information <b>CVE ID : CVE-2023- 27954</b>	ort.apple.co m/en- us/HT21367 3, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 8, https://supp ort.apple.co m/en- us/HT21367 6	
N/A	08-May-2023	5.5	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. Processing maliciously crafted web content may bypass Same Origin Policy <b>CVE ID : CVE-2023- 27932</b>	https://supp ort.apple.co m/en- us/HT21367 4, https://supp ort.apple.co m/en- us/HT21367 0, https://supp ort.apple.co m/en- us/HT21367 1, https://supp ort.apple.co m/en- us/HT21367 8,	O-DEB-DEBI- 170523/1788

0-1

1-2

3-4 4-5 2-3 Page 766 of 1106

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://supp ort.apple.co m/en- us/HT21367 6	
Affected Ver	sion(s): 11.0			I	
Use After Free	03-May-2023	8.8	Use after free in OS Inputs in Google Chrome on ChromeOS prior to 113.0.5672.63 allowed a remote attacker who convinced a user to enage in specific UI interaction to potentially exploit heap corruption via crafted UI interaction. (Chromium security severity: Medium) <b>CVE ID : CVE-2023-</b> 2461	N/A	O-DEB-DEBI- 170523/1789
Improper Input Validation	03-May-2023	7.1	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to bypass file access checks via a crafted HTML page. (Chromium security severity: Medium) <b>CVE ID : CVE-2023- 2460</b>	N/A	O-DEB-DEBI- 170523/1790

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-May-2023	6.5	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to bypass permission restrictions via a crafted HTML page. (Chromium security severity: Medium) <b>CVE ID : CVE-2023-</b> 2459	N/A	O-DEB-DEBI- 170523/1791
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to obfuscate main origin data via a crafted HTML page. (Chromium security severity: Medium) <b>CVE ID : CVE-2023-</b> 2462	N/A	O-DEB-DEBI- 170523/1792
N/A	03-May-2023	4.3	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	N/A	O-DEB-DEBI- 170523/1793

0-1

1-2

**2-3** 3-4 4-5 Page **768** of **1106**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 2463		
N/A	03-May-2023	4.3	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to perform an origin spoof in the security UI via a crafted HTML page. (Chromium security severity: Medium) <b>CVE ID : CVE-2023-</b>	N/A	O-DEB-DEBI- 170523/1794
N/A	03-May-2023	4.3	2464 Inappropriate implementation in CORS in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) CVE ID : CVE-2023- 2465	N/A	O-DEB-DEBI- 170523/1795
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to spoof the contents of the security UI via a crafted HTML page.	N/A	O-DEB-DEBI- 170523/1796

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			(Chromium security severity: Low) CVE ID : CVE-2023- 2466						
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to bypass permissions restrictions via a crafted HTML page. (Chromium security severity: Low) <b>CVE ID : CVE-2023-</b> 2467	N/A	O-DEB-DEBI- 170523/1797				
N/A	03-May-2023	4.3	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed a remote attacker who had compromised the renderer process to obfuscate the security UI via a crafted HTML page. (Chromium security severity: Low) <b>CVE ID : CVE-2023-</b> <b>2468</b>	N/A	O-DEB-DEBI- 170523/1798				
Vendor: Dli	Vendor: Dlink								
Product: dir-868l_firmware									
	sion(s): 1.12								
Buffer Copy without	02-May-2023	9.8	** UNSUPPORTED WHEN ASSIGNED ** D-Link DIR-868L	https://ww w.dlink.com/ en/security-	O-DLI-DIR 170523/1799				
CVSS Scoring	Scale 0-1	L-2 2-3	3-4 4-5 5-6	6-7 7-8	8 8-9 9-10				

Page 770 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Checking Size of Input ('Classic Buffer Overflow')			Hardware version A1, firmware version 1.12 is vulnerable to Buffer Overflow. The vulnerability is in scandir.sgi binary. <b>CVE ID : CVE-2023- 29856</b>	bulletin/, https://supp ortannounce ment.us.dlin k.com/anno uncement/p ublication.as px?name=SA P10325		
Product: dir	-879_firmware					
Affected Vers	sion(s): 1.10					
Improper Authentica tion	01-May-2023	7.5	D-Link DIR-879 v105A1 is vulnerable to Authentication Bypass via phpcgi. CVE ID : CVE-2023- 30061	https://ww w.dlink.com/ en/security- bulletin/	O-DLI-DIR 170523/1800	
Product: dir	r-890l_firmware	e				
Affected Vers	sion(s): 1.05					
Improper Authentica tion	01-May-2023	7.5	D-Link DIR-890L FW1.10 A1 is vulnerable to Authentication bypass. <b>CVE ID : CVE-2023-</b> <b>30063</b>	https://ww w.dlink.com/ en/security- bulletin/	O-DLI-DIR 170523/1801	
Vendor: ez-	net					
Product: ne	xt-7004n_firmw	are				
Affected Vers	sion(s): 3.0.1					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	6.1	A vulnerability was found in NEXTU NEXT-7004N 3.0.1. It has been classified as problematic. Affected is an unknown function of the file /boafrm/formFilter of the component POST Request	N/A	0-EZNEXT- 170523/1802	
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10						

Page 771 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Handler. The manipulation of the argument url with the input <svg onload=alert(1337)&gt; leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB- 228012. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. <b>CVE ID : CVE-2023-</b> <b>2521</b></svg 		
Vendor: Fed	loraproiect		2321		
Product: fee					
Affected Ver	sion(s): 36				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user- supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database. <b>CVE ID : CVE-2023- 30944</b>	https://moo dle.org/mod /forum/disc uss.php?d=4 46286, https://bugz illa.redhat.co m/show_bug .cgi?id=2188 606, http://git.m oodle.org/g w?p=moodle .git&a=searc h&h=HEAD& st=commit& s=MDL- 77187	0-FED-FEDO- 170523/1803

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Divide By Zero	05-May-2023	6.5	A Segmentation fault caused by a floating point exception exists in libheif 1.15.1 using crafted heif images via the heif::Fraction::round () function in box.cc, which causes a denial of service. <b>CVE ID : CVE-2023- 29659</b>	N/A	0-FED-FEDO- 170523/1804
Externally Controlled Reference to a Resource in Another Sphere	02-May-2023	5.3	The vulnerability was found Moodle which exists because the application allows a user to control path of the older to create in TinyMCE loaders. A remote user can send a specially crafted HTTP request and create arbitrary folders on the system. <b>CVE ID : CVE-2023-</b> <b>30943</b>	http://git.m oodle.org/g w?p=moodle .git&a=searc h&h=HEAD& st=commit& s=MDL- 77718, https://moo dle.org/mod /forum/disc uss.php?d=4 46285, https://bugz illa.redhat.co m/show_bug .cgi?id=2188 605	0-FED-FEDO- 170523/1805
Affected Ver	sion(s): 37				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user- supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the	https://moo dle.org/mod /forum/disc uss.php?d=4 46286, https://bugz illa.redhat.co m/show_bug .cgi?id=2188 606, http://git.m oodle.org/g	0-FED-FEDO- 170523/1806
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5-6	5 6-7 7-8	8 8-9 9-10

3-4 4-5 2-3 Page 773 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected application and execute limited SQL commands within the application database. CVE ID : CVE-2023- 30944	w?p=moodle .git&a=searc h&h=HEAD& st=commit& s=MDL- 77187	
Divide By Zero	05-May-2023	6.5	A Segmentation fault caused by a floating point exception exists in libheif 1.15.1 using crafted heif images via the heif::Fraction::round () function in box.cc, which causes a denial of service. <b>CVE ID : CVE-2023-</b>	N/A	O-FED-FEDO- 170523/1807
Externally Controlled Reference to a Resource in Another Sphere	02-May-2023	5.3	29659 The vulnerability was found Moodle which exists because the application allows a user to control path of the older to create in TinyMCE loaders. A remote user can send a specially crafted HTTP request and create arbitrary folders on the system. CVE ID : CVE-2023- 30943	http://git.m oodle.org/g w?p=moodle .git&a=searc h&h=HEAD& st=commit& s=MDL- 77718, https://moo dle.org/mod /forum/disc uss.php?d=4 46285, https://bugz illa.redhat.co m/show_bug .cgi?id=2188 605	O-FED-FEDO- 170523/1808
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63	N/A	O-FED-FEDO- 170523/1809

0-1

1-2

**2-3** 3-4 4-5 Page **774** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed a remote attacker to obfuscate main origin data via a crafted HTML page. (Chromium security severity: Medium)		
			CVE ID : CVE-2023- 2462		
Affected Ver	sion(s): 38				
Improper Input Validation	07-May-2023	9.8	In Django 3.2 before 3.2.19, 4.x before 4.1.9, and 4.2 before 4.2.1, it was possible to bypass validation when using one form field to upload multiple files. This multiple upload has never been supported by forms.FileField or forms.ImageField (only the last uploaded file was validated). However, Django's "Uploading multiple files" documentation suggested otherwise. <b>CVE ID : CVE-2023- 31047</b>	https://ww w.djangoproj ect.com/web log/2023/m ay/03/secur ity-releases/, https://docs. djangoprojec t.com/en/4. 2/releases/s ecurity/	O-FED-FEDO- 170523/1810
Use After Free	03-May-2023	8.8	Use after free in OS Inputs in Google Chrome on ChromeOS prior to 113.0.5672.63 allowed a remote attacker who convinced a user to enage in specific UI interaction to potentially exploit	N/A	O-FED-FEDO- 170523/1811

0-1

1-2

2-33-44-5Page 775 of 1106

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			heap corruption via crafted UI interaction. (Chromium security severity: Medium)		
			CVE ID : CVE-2023- 2461		
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user- supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database. <b>CVE ID : CVE-2023- 30944</b>	https://moo dle.org/mod /forum/disc uss.php?d=4 46286, https://bugz illa.redhat.co m/show_bug .cgi?id=2188 606, http://git.m oodle.org/g w?p=moodle .git&a=searc h&h=HEAD& st=commit& s=MDL- 77187	O-FED-FEDO- 170523/1812
Improper Input Validation	03-May-2023	7.1	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to bypass file access checks via a crafted HTML page. (Chromium security severity: Medium)	N/A	0-FED-FEDO- 170523/1813

0-1

1-2

2-33-44-5Page 776 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 2460		
N/A	03-May-2023	6.5	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to bypass permission restrictions via a crafted HTML page. (Chromium security severity: Medium) CVE ID : CVE-2023- 2459	N/A	O-FED-FEDO- 170523/1814
Externally Controlled Reference to a Resource in Another Sphere	02-May-2023	5.3	The vulnerability was found Moodle which exists because the application allows a user to control path of the older to create in TinyMCE loaders. A remote user can send a specially crafted HTTP request and create arbitrary folders on the system. <b>CVE ID : CVE-2023-</b> <b>30943</b>	http://git.m oodle.org/g w?p=moodle .git&a=searc h&h=HEAD& st=commit& s=MDL- 77718, https://moo dle.org/mod /forum/disc uss.php?d=4 46285, https://bugz illa.redhat.co m/show_bug .cgi?id=2188 605	O-FED-FEDO- 170523/1815
N/A	03-May-2023	4.3	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to hide the contents of the	N/A	O-FED-FEDO- 170523/1816

0-1

1-2

2-33-44-5Page 777 of 1106

5-6

7-8

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)		
			CVE ID : CVE-2023- 2463		
N/A	03-May-2023	4.3	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to perform an origin spoof in the security UI via a crafted HTML page. (Chromium security severity: Medium) <b>CVE ID : CVE-2023-</b> <b>2464</b>	N/A	0-FED-FEDO- 170523/1817
N/A	03-May-2023	4.3	Inappropriate implementation in CORS in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) <b>CVE ID : CVE-2023-</b> <b>2465</b>	N/A	0-FED-FEDO- 170523/1818
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63	N/A	0-FED-FEDO- 170523/1819

0-1

1-2

**2-3** 3-4 4-5 Page **778** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			allowed a remote attacker to spoof the contents of the security UI via a crafted HTML page. (Chromium security severity: Low)				
			CVE ID : CVE-2023- 2466				
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to bypass permissions restrictions via a crafted HTML page. (Chromium security severity: Low) <b>CVE ID : CVE-2023-</b> 2467	N/A	O-FED-FEDO- 170523/1820		
N/A	03-May-2023	4.3	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed a remote attacker who had compromised the renderer process to obfuscate the security UI via a crafted HTML page. (Chromium security severity: Low) <b>CVE ID : CVE-2023- 2468</b>	N/A	O-FED-FEDO- 170523/1821		
Vendor: feiyuxing							

0-1

1-2

**2-3** 3-4 4-5 Page **779** of **1106**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Product: ve	c40g_firmware		I		I	
Affected Ver	sion(s): 3.0					
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	04-May-2023	7.2	A vulnerability was found in Chengdu VEC40G 3.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /send_order.cgi?para meter=access_detect of the component Network Detection. The manipulation of the argument COUNT with the input 3   netstat - an leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB- 228013 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. <b>CVE ID : CVE-2023- 2522</b>	N/A	O-FEI-VEC4- 170523/1822	
Vendor: fiio Product: m6_firmware						
Affected ver	sion(s): 1.0.4					

0-1

1-2

**2-3** 3-4 4-5 Page **780** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	7.8	A buffer overflow in the component /proc/ftxxxx-debug of FiiO M6 Build Number v1.0.4 allows attackers to escalate privileges to root. <b>CVE ID : CVE-2023-</b> <b>30257</b>	N/A	0-FII-M6_F- 170523/1823
Vendor: For	tinet			I	
Product: for	rtios				
Affected Ver	sion(s): From (in	cluding) 6	.0.0 Up to (including) 6	.0.16	
Out-of- bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via	https://forti guard.com/p sirt/FG-IR- 22-475	O-FOR-FORT- 170523/1824

0-1

1-2

2-33-44-5Page 781 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specifically crafted requests.		
			CVE ID : CVE-2023- 22640		
Affected Vers	sion(s): From (in	cluding) 6	.2.0 Up to (excluding) 6	.2.14	
Out-of- bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests. <b>CVE ID : CVE-2023- 22640</b>	https://forti guard.com/p sirt/FG-IR- 22-475	0-F0R-F0RT- 170523/1825
Out-of- bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3,	https://forti guard.com/p sirt/FG-IR- 22-475	O-FOR-FORT- 170523/1826
CVSS Scoring S	icale 0-1 i	L-2 2-3	3-4 4-5 5-6 Page <b>782</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSSv3	FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted	Patch	NCIIPC ID
			requests. CVE ID : CVE-2023-		
			22640		
Affected Ver	sion(s): From (in	cluding) 7	.0.0 Up to (excluding) 7	.0.11	
Out-of- bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1,	https://forti guard.com/p sirt/FG-IR- 22-475	0-FOR-FORT- 170523/1827

0-1

1-2

3-4 4-5 2-3 Page 783 of 1106

5-6

6-7

8-9 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests.		
			CVE ID : CVE-2023- 22640		
Affected Ver	sion(s): From (in	cluding) 7	.2.0 Up to (excluding) 7	.2.4	
Out-of- bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows	https://forti guard.com/p sirt/FG-IR- 22-475	0-FOR-FORT- 170523/1828

0-1

1-2

**2-3** 3-4 4-5 Page **784** of **1106**  5-6

6-7

			an authenticated				
			attacker to execute unauthorized code or commands via specifically crafted requests.				
			CVE ID : CVE-2023- 22640				
Vendor: garo	)						
Product: wal	llbox_glb_firmw	vare					
Affected Versi	ion(s): * Up to (i	ncluding)	189				
Incorrect Permission Assignmen t for Critical Resource	04-May-2023	8.1	Insecure permissions in the settings page of GARO Wallbox GLB/GTB/GTC before v189 allows attackers to redirect users to a crafted update package link via a man-in-the- middle attack.	N/A	0-GAR-WALL- 170523/1829		
			CVE ID : CVE-2023- 30399				
Product: wal	llbox_gtb_firmw	are					
Affected Versi	ion(s): * Up to (i	ncluding)	189				
Incorrect Permission Assignmen t for Critical Resource	04-May-2023	8.1	Insecure permissions in the settings page of GARO Wallbox GLB/GTB/GTC before v189 allows attackers to redirect users to a crafted update package link via a man-in-the- middle attack. <b>CVE ID : CVE-2023- 30399</b>	N/A	0-GAR-WALL- 170523/1830		
Product: wallbox_gtc_firmware							
Affected Versi	ion(s): * Up to (i	ncluding)	189				

0-1

1-2

**2-3** 3-4 4-5 Page **785** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Incorrect Permission Assignmen t for Critical Resource	04-May-2023	8.1	Insecure permissions in the settings page of GARO Wallbox GLB/GTB/GTC before v189 allows attackers to redirect users to a crafted update package link via a man-in-the- middle attack. <b>CVE ID : CVE-2023-</b> 30399	N/A	O-GAR-WALL- 170523/1831			
Vendor: gl-i	net							
Product: gl-	mt3000_firmwa	ire						
Affected Ver	sion(s): 4.1.0							
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	02-May-2023	9.8	GL.iNET MT3000 4.1.0 Release 2 is vulnerable to OS Command Injection via /usr/lib/oui- httpd/rpc/logread. <b>CVE ID : CVE-2023- 29778</b>	N/A	0-GLGL-M- 170523/1832			
Vendor: Goo	ogle			I				
Product: an	droid							
Affected Ver	sion(s): -							
N/A	03-May-2023	4.3	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium	N/A	0-GOO-ANDR- 170523/1833			
	pugor (on onnum							
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10           Page 786 of 1106								

Page **786** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			security severity: Medium) CVE ID : CVE-2023- 2463				
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to bypass permissions restrictions via a crafted HTML page. (Chromium security severity: Low)	N/A	0-GOO-ANDR- 170523/1834		
			CVE ID : CVE-2023- 2467				
Product: ch							
Affected Ver	sion(s): -				1		
Use After Free	03-May-2023	8.8	Use after free in OS Inputs in Google Chrome on ChromeOS prior to 113.0.5672.63 allowed a remote attacker who convinced a user to enage in specific UI interaction to potentially exploit heap corruption via crafted UI interaction. (Chromium security severity: Medium) <b>CVE ID : CVE-2023-</b> <b>2461</b>	N/A	O-GOO-CHRO- 170523/1835		
Vendor: H3	C		2101				
Product: gr-1200w_firmware							
CVSS Scoring	Scale 0-1	1-2 2-3	<b>3 3-4 4-5 5-6</b> Page <b>787</b> of <b>1106</b>	5 <u>6-7</u> 7-	8 8-9 <mark>9-10</mark>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): minigrw	1a0v100r	006		
Out-of- bounds Write	08-May-2023	9.8	H3C GR-1200W MiniGRW1A0V100R 006 was discovered to contain a stack overflow via the function set_tftp_upgrad. CVE ID : CVE-2023- 29693	N/A	0-H3C-GR-1- 170523/1836
Out-of- bounds Write	08-May-2023	9.8	H3C GR-1200W MiniGRW1A0V100R 006 was discovered to contain a stack overflow via the function version_set. CVE ID : CVE-2023- 29696	N/A	0-H3C-GR-1- 170523/1837
Vendor: HP					
Product: ar	ubaos				
Affected Ver	sion(s): From (in	cluding) 1	0.3.0.0 Up to (including	g) 10.3.1.0	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-ARUB- 170523/1838

0-1

1-2

**2-3** 3-4 4-5 Page **788** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	22779 There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22780</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-ARUB- 170523/1839
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-ARUB- 170523/1840

0-1

1-2

**2-3** 3-4 4-5 Page **789** of **1106**  7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b> <b>22781</b>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22782</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-ARUB- 170523/1841

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22783</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-ARUB- 170523/1842
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-ARUB- 170523/1843

0-1

1-2

2-33-44-5Page 791 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.		
			CVE ID : CVE-2023- 22784		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b> <b>22785</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-ARUB- 170523/1844
Buffer Copy without Checking Size of Input ('Classic	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-ARUB- 170523/1845

0-1

1-2

2-33-44-5Page 792 of 1106

5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22786</b>		
Product: ins					
Affected Ver	sion(s): From (in	cluding) 6	.4.0.0 Up to (including) There are buffer	6.4.4.8-4.2.4.20	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1846

0-1

1-2

2-3 3-4 4-5 Page **793** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system. CVE ID : CVE-2023- 22779		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1847
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	22780 There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1848

0-1

1-2

**2-3** 3-4 4-5 Page **794** of **1106**  8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b> <b>22781</b>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22782</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1849
Buffer Copy without Checking	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying	https://ww w.arubanetw orks.com/as sets/alert/A	0-HP-INST- 170523/1850

0-1

1-2

2-3 3-4 4-5 Page **795** of **1106**  6-7

5-6

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22783</b>	RUBA-PSA- 2023-006.txt	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1851

0-1

1-2

2-3 3-4 4-5 Page **796** of **1106**  6-7

7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system. <b>CVE ID : CVE-2023-</b> <b>22784</b>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22785</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1852
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1853

0-1

1-2

2-3 3-4 4-5 Page **797** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b> <b>22786</b>		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1854
Improper Neutralizat ion of Special Elements used in a Command ('Comman	08-May-2023	8.8	22788 Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface.	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1855

0-1

1-2

**2-3** 3-4 4-5 Page **798** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b> <b>22789</b>		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22790</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1856
N/A	08-May-2023	7.5	An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1857

0-1

1-2

2-3 3-4 4-5 Page **799** of **1106**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the ability to interrupt the normal operation of the affected access point. <b>CVE ID : CVE-2023-</b>		
			22787		
N/A	08-May-2023	4.8	A vulnerability exists in Aruba InstantOS and ArubaOS 10 where an edge- case combination of network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of potentially sensitive information can occur are complex and depend on factors that are beyond the control of the attacker. <b>CVE ID : CVE-2023-</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1858
Affected Ver	sion(s): From (in	cluding) 6	22791 .5.0.0 Up to (including)	65423	
Buffer Copy without Checking Size of Input ('Classic	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1859

0-1

1-2

**2-3** 3-4 4-5 Page **800** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	22779 There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1860

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22780		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22781</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1861
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211).	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1862

0-1

1-2

**2-3** 3-4 4-5 Page **802** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	22782 There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22783</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1863
Buffer Copy without Checking Size of Input	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to	https://ww w.arubanetw orks.com/as sets/alert/A	O-HP-INST- 170523/1864

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22784</b>	RUBA-PSA- 2023-006.txt	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1865

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system. CVE ID : CVE-2023- 22785		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22786</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1866
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1867

0-1

1-2

**2-3** 3-4 4-5 Page **805** of **1106**  5-6

9-10

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands as a privileged user on the underlying operating system.		
			CVE ID : CVE-2023- 22788		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1868
			CVE ID : CVE-2023- 22789		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1869

0-1

1-2

**2-3** 3-4 4-5 Page **806** of **1106**  8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system.		
			CVE ID : CVE-2023- 22790		
N/A	08-May-2023	7.5	An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point.	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1870
			CVE ID : CVE-2023- 22787		
N/A	08-May-2023	4.8	A vulnerability exists in Aruba InstantOS and ArubaOS 10 where an edge- case combination of network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of potentially sensitive information can occur are complex	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1871

0-1

1-2

**2-3** 3-4 4-5 Page **807** of **1106**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and depend on factors that are beyond the control of the attacker.		
			CVE ID : CVE-2023- 22791		
Affected Ver	sion(s): From (in	cluding) 8	.10.0.0 Up to (including	) 8.10.0.4	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1872
			CVE ID : CVE-2023- 22779		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1873

0-1

1-2

**2-3** 3-4 4-5 Page **808** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b> <b>22780</b>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22781</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1874

0-1

1-2

**2-3** 3-4 4-5 Page **809** of **1106**  5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22782</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1875
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1876

0-1

1-2

**2-3** 3-4 4-5 Page **810** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.		
			CVE ID : CVE-2023- 22783		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22784</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1877
Buffer Copy without Checking Size of Input ('Classic	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1878

0-1

1-2

2-33-44-5Page 811 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	22785 There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1879

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22786		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22788</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1880
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22789</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1881

0-1

1-2

2-33-44-5Page 813 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22790</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1882
N/A	08-May-2023	7.5	An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point. <b>CVE ID : CVE-2023- 22787</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1883
N/A	08-May-2023	4.8	A vulnerability exists in Aruba InstantOS and ArubaOS 10 where an edge- case combination of	https://ww w.arubanetw orks.com/as sets/alert/A	0-HP-INST- 170523/1884

0-1

1-2

**2-3** 3-4 4-5 Page **814** of **1106**  6-7

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of potentially sensitive information can occur are complex and depend on factors that are beyond the control of the attacker. <b>CVE ID : CVE-2023-</b> <b>22791</b>	RUBA-PSA- 2023-006.txt	
Affected Ver	sion(s): From (in	cluding) 8	.4.0.0 Up to (excluding)	8.6.0.0	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1885

0-1

1-2

2-33-44-5Page 815 of 1106

5-6

6-7

7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	22779 There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22780</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1886
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1887

0-1

1-2

**2-3** 3-4 4-5 Page **816** of **1106**  7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b> 22781		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22782</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1888

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22783</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1889
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1890

0-1

1-2

**2-3** 3-4 4-5 Page **818** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.		
			CVE ID : CVE-2023- 22784		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b> <b>22785</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1891
Buffer Copy without Checking Size of Input ('Classic	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1892

0-1

1-2

**2-3** 3-4 4-5 Page **819** of **1106**  7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22786</b>		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1893
Improper Neutralizat ion of Special Elements	08-May-2023	8.8	<b>22788</b> Multiple authenticated command injection vulnerabilities exist in the Aruba	https://ww w.arubanetw orks.com/as sets/alert/A	O-HP-INST- 170523/1894

0-1

1-2

**2-3** 3-4 4-5 Page **820** of **1106**  5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Comman d Injection')			InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22789</b>	RUBA-PSA- 2023-006.txt	
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1895
N/A	08-May-2023	7.5	22790 An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1896

0-1

1-2

2-33-44-5Page 821 of 1106

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point.		
			CVE ID : CVE-2023- 22787		
N/A	08-May-2023	4.8	A vulnerability exists in Aruba InstantOS and ArubaOS 10 where an edge- case combination of network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of potentially sensitive information can occur are complex and depend on factors that are beyond the control of the attacker. <b>CVE ID : CVE-2023- 22791</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1897
Affected Ver	sion(s): From (in	cluding) 8	.6.0.0 Up to (including)	8.6.0.19	
Buffer Copy without Checking	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying	https://ww w.arubanetw orks.com/as sets/alert/A	0-HP-INST- 170523/1898

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22779</b>	RUBA-PSA- 2023-006.txt	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1899

0-1

1-2

2-33-44-5Page 823 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system. CVE ID : CVE-2023- 22780		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b> <b>22781</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1900
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1901

0-1

1-2

**2-3** 3-4 4-5 Page **824** of **1106**  5-6

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b> <b>22782</b>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22783</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1902
Buffer Copy without	08-May-2023	9.8	There are buffer overflow vulnerabilities in	https://ww w.arubanetw orks.com/as	0-HP-INST- 170523/1903

0-1

1-2

3-4 4-5 2-3 Page 825 of 1106

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22784</b>	sets/alert/A RUBA-PSA- 2023-006.txt	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1904

0-1

1-2

**2-3** 3-4 4-5 Page **826** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b>		
			22785		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22786</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1905
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1906

0-1

1-2

**2-3** 3-4 4-5 Page **827** of **1106**  5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.		
			CVE ID : CVE-2023- 22788		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22789</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1907
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1908

0-1

1-2

**2-3** 3-4 4-5 Page **828** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b> <b>22790</b>		
N/A	08-May-2023	7.5	An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point. <b>CVE ID : CVE-2023-</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1909
N/A	08-May-2023	4.8	22787 A vulnerability exists in Aruba InstantOS and ArubaOS 10 where an edge- case combination of network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of potentially sensitive	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1910

0-1

1-2

**2-3** 3-4 4-5 Page **829** of **1106**  5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information can occur are complex and depend on factors that are beyond the control of the attacker.		
			CVE ID : CVE-2023- 22791		
Affected Ver	sion(s): From (in	cluding) 8	8.7.0.0 Up to (including)	8.9.0.0	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22779</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1911
Buffer Copy without Checking Size of Input ('Classic	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1912

0-1

1-2

**2-3** 3-4 4-5 Page **830** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b> 22780		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1913

0-1

1-2

**2-3** 3-4 4-5 Page **831** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22781		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b> <b>22782</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1914
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211).	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1915

0-1

1-2

2-33-44-5Page 832 of 1106

5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	22783 There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. CVE ID : CVE-2023- 22784	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1916
Buffer Copy without Checking Size of Input	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to	https://ww w.arubanetw orks.com/as sets/alert/A	O-HP-INST- 170523/1917

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22785</b>	RUBA-PSA- 2023-006.txt	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	O-HP-INST- 170523/1918

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system. CVE ID : CVE-2023- 22786		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023- 22788</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1919
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1920

0-1

1-2

**2-3** 3-4 4-5 Page **835** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22789		
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. <b>CVE ID : CVE-2023-</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1921
N/A	08-May-2023	7.5	22790 An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point. <b>CVE ID : CVE-2023- 22787</b>	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	0-HP-INST- 170523/1922
N/A	08-May-2023	4.8	A vulnerability exists in Aruba InstantOS	https://ww w.arubanetw	0-HP-INST- 170523/1923

0-1

1-2

**2-3** 3-4 4-5 Page **836** of **1106**  5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and ArubaOS 10 where an edge- case combination of network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of potentially sensitive information can occur are complex and depend on factors that are beyond the control of the attacker. <b>CVE ID : CVE-2023- 22791</b>	orks.com/as sets/alert/A RUBA-PSA- 2023-006.txt	
Product: int	tegrated_lights-o	out_firmw	vare		
Affected Ver	sion(s): 1.05				
N/A	01-May-2023	6.8	A potential security vulnerability has been identified in HPE ProLiant RL300 Gen11 Server. The vulnerability could result in the system being vulnerable to exploits by attackers with physical access inside the server chassis.	https://supp ort.hpe.com/ hpesc/public /docDisplay? docLocale=e n_US&docId =hpesbhf044 72en_us	O-HP-INTE- 170523/1924

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 28092		
Product: pr	oliant_rl300_fir	mware			
Affected Ver	sion(s): 1.12				
N/A	01-May-2023	6.8	A potential security vulnerability has been identified in HPE ProLiant RL300 Gen11 Server. The vulnerability could result in the system being vulnerable to exploits by attackers with physical access inside the server chassis.	https://supp ort.hpe.com/ hpesc/public /docDisplay? docLocale=e n_US&docId =hpesbhf044 72en_us	O-HP-PROL- 170523/1925
Vendor: IBN	Л		CVE ID : CVE-2023- 28092		
	48-ved_firmwai	10			
			.53.0 Up to (including)	8.53.0.63	
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X- Force ID: 246320. <b>CVE ID : CVE-2023-</b> 24958	https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24632 0, https://ww w.ibm.com/s upport/page s/node/698 0845	O-IBM-3948- 170523/1926

0-1

1-2

**2-3** 3-4 4-5 Page **838** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Product: 39	57-vec_firmwar	е					
Affected Ver	sion(s): From (in	cluding) 8	8.51.0 Up to (excluding)	8.51.2.12			
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X- Force ID: 246320.	https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24632 0, https://ww w.ibm.com/s upport/page s/node/698 0845	0-IBM-3957- 170523/1927		
			CVE ID : CVE-2023- 24958				
Attected Ver	sion(s): From (in	cluding) 8	.52.100.0 Up to (exclud	ing) 8.52.102.1	3		
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X- Force ID: 246320. <b>CVE ID : CVE-2023-</b>	https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24632 0, https://ww w.ibm.com/s upport/page s/node/698 0845	0-IBM-3957- 170523/1928		
Droduct. 20	E7 und firmura		24958				
Product: 3957-ved_firmware Affected Version(s): From (including) 8.51.0 Up to (excluding) 8.51.2.12							
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700	https://exch ange.xforce.i	O-IBM-3957- 170523/1929		
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 839 of 1106						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X- Force ID: 246320.	bmcloud.co m/vulnerabi lities/24632 0, https://ww w.ibm.com/s upport/page s/node/698 0845	
			CVE ID : CVE-2023- 24958		
Affected Ver	sion(s): From (in	cluding) 8	.52.100.0 Up to (exclud	ing) 8.52.102.13	3
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X- Force ID: 246320. <b>CVE ID : CVE-2023-</b> 24958	https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24632 0, https://ww w.ibm.com/s upport/page s/node/698 0845	O-IBM-3957- 170523/1930
Affected Ver	sion(s): From (in	cluding) 8	.52.200.0 Up to (exclud	ing) 8.52.200.12	11
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated	https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24632 0, https://ww w.ibm.com/s	O-IBM-3957- 170523/1931

0-1

1-2

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X- Force ID: 246320. <b>CVE ID : CVE-2023-</b> <b>24958</b>	upport/page s/node/698 0845	
Affected Ver	sion(s): From (in	cluding) 8	.53.0 Up to (excluding)	8.53.0.63	
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X- Force ID: 246320.	https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24632 0, https://ww w.ibm.com/s upport/page s/node/698 0845	0-IBM-3957- 170523/1932
			CVE ID : CVE-2023- 24958		
Product: i					
Affected Ver	sion(s): 7.2				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	04-May-2023	7.2	IBM i 7.2, 7.3, 7.4, and 7.5 could allow an authenticated privileged administrator to gain elevated privileges in non-default configurations, as a result of improper SQL processing. By using a specially crafted SQL operation, the	https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24451 0, https://ww w.ibm.com/s upport/page s/node/698 7767	0-IBM-I- 170523/1933
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5-6	6-7 7-8	3 8-9 <mark>9-1</mark> 0

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator could exploit the vulnerability to perform additional administrator operations. IBM X- Force ID: 244510.		
			CVE ID : CVE-2023- 23470		
Affected Ver	sion(s): 7.3				
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	04-May-2023	7.2	IBM i 7.2, 7.3, 7.4, and 7.5 could allow an authenticated privileged administrator to gain elevated privileges in non-default configurations, as a result of improper SQL processing. By using a specially crafted SQL operation, the administrator could exploit the vulnerability to perform additional administrator operations. IBM X- Force ID: 244510. <b>CVE ID : CVE-2023- 23470</b>	https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24451 0, https://ww w.ibm.com/s upport/page s/node/698 7767	O-IBM-I- 170523/1934
Affected Ver	sion(s): 7.4				
Improper Neutralizat ion of Special Elements used in an SQL Command	04-May-2023	7.2	IBM i 7.2, 7.3, 7.4, and 7.5 could allow an authenticated privileged administrator to gain elevated privileges in non-default configurations, as a result of improper	https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24451 0, https://ww w.ibm.com/s upport/page	O-IBM-I- 170523/1935

0-1

1-2

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
('SQL Injection')			SQL processing. By using a specially crafted SQL operation, the administrator could exploit the vulnerability to perform additional administrator operations. IBM X- Force ID: 244510. CVE ID : CVE-2023- 23470	s/node/698 7767		
Affected Vers	sion(s): 7.5					
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')	04-May-2023	7.2	IBM i 7.2, 7.3, 7.4, and 7.5 could allow an authenticated privileged administrator to gain elevated privileges in non-default configurations, as a result of improper SQL processing. By using a specially crafted SQL operation, the administrator could exploit the vulnerability to perform additional administrator operations. IBM X- Force ID: 244510. <b>CVE ID : CVE-2023- 23470</b>	https://exch ange.xforce.i bmcloud.co m/vulnerabi lities/24451 0, https://ww w.ibm.com/s upport/page s/node/698 7767	O-IBM-I- 170523/1936	
Vendor: kai						
Product: kaios Affected Version(s): 3.0						
N/A	01-May-2023	5.3	An issue was discovered in KaiOS	N/A	0-KAI-KAIO- 170523/1937	

Page 843 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			3.0. The pre-installed Communications application exposes a Web Activity that returns the user's call log without origin or permission checks. An attacker can inject a JavaScript payload that runs in a browser or app without user interaction or consent. This allows an attacker to send the user's call logs to a remote server via XMLHttpRequest or Fetch. <b>CVE ID : CVE-2023-</b>						
Vendor: Ler			27108						
		tial with	_alexa_built_in_firmwa	nre					
	sion(s): * Up to (e								
N/A	01-May-2023	8.8	A default password was reported in Lenovo Smart Clock Essential with Alexa Built In that could allow unauthorized device access to an attacker with local network access. <b>CVE ID : CVE-2023- 0896</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 113714	0-LEN-SMAR- 170523/1938				
Product: thi	Product: thinkagile_hx1021_firmware								
Affected Ver	sion(s): * Up to (e	excluding)	3.72_tei388s						
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only	https://supp ort.lenovo.co m/us/en/pr	0-LEN-THIN- 170523/1939				
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>844</b> of <b>1106</b>	6-7 7-8	<u>8 8-9 9-10</u>				

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access may gain elevated privileges through a specifically crafted API call.	oduct_securi ty/LEN- 99936	
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1940
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx1320	_firmwaı	'e		
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a		
N/A	01-May-2023	01-May-2023 8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/1941
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1942

0-1

1-2

**2-3** 3-4 4-5 Page **845** of **1106**  5-6

6-7

		vulnerability in a web interface API.		
		CVE ID : CVE-2023- 25492		
inkagile_hx1321	_firmwaı	'e		
sion(s): * Up to (e	excluding)	8.88_cdi3a4a		
01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/1943
01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1944
		25492		
6				
sion(s): * Up to (e	excluding)	- *		
01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1945
	sion(s): * Up to (e 01-May-2023 01-May-2023 inkagile_hx1331 sion(s): * Up to (e	sion(s): * Up to (excluding) 01-May-2023 8.8 01-May-2023 8.8 inkagile_hx1331_firmwar sion(s): * Up to (excluding)	Image:	ImageCVE ID : CVE-2023- 25492inkagile_hx1321_firmwaresion(s):* Up to (excluding)01-May-20238.801-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.01-May-202301-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. CVE ID : CVE-2023- 25492inkagile_hx1331_firmware01-May-20238.801-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privileges through a format string injection vulnerability in a web interface API. CVE ID : CVE-2023- 2549201-May-20238.801-May-20238.88.8A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.01-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.01-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.01-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privile

0-1

1-2

**2-3** 3-4 4-5 Page **846** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1946		
			CVE ID : CVE-2023- 25492				
Product: thi	inkagile_hx152(	)-r_firmw	are	I			
Affected Ver	sion(s): * Up to (	excluding)	8.88_cdi3a4a				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1947		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/1948		
Droduct, thi	intragila hy1521	n firmu	25492				
Product: thinkagile_hx1521-r_firmware Affected Version(s): * Up to (excluding) 8.88_cdi3a4a							
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3 3-4 4-5 5-6</b> Page <b>847</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/1949
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1950
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx2320	)-e_firmw	are		
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023-	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1951
			0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1952

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			behavior through a format string injection vulnerability in a web interface API.					
			CVE ID : CVE-2023- 25492					
Product: thi	inkagile_hx2321	_firmwaı	re	<u> </u>				
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a					
N/A	01-May-2023	1-May-2023 8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1953			
			CVE ID : CVE-2023- 0683					
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1954			
			CVE ID : CVE-2023- 25492					
	Product: thinkagile_hx2330_firmware							
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p	1				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1955			

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b> <b>25492</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/1956
Affected Ver	sion(s): 2.93_afbt	:30p			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1957
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1958

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx2331	_firmwai	re		
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1959
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1960
			25492		
Product: thi	inkagile_hx272(	)-e_firmw	are	·	·
Affected Ver	sion(s): * Up to (e	excluding)	3.72_tei388s		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1961
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	O-LEN-THIN- 170523/1962

0-1

1-2

2-33-44-5Page 851 of 1106

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936	
Product: thi	inkagile_hx3320	_firmwai	'e		
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1963
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/1964
			25492		
	inkagile_hx3321				
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a		

0-1

1-2

2-33-44-5Page 852 of 1106

5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1965
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/1966
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx3330	_firmwai	re		
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1967
			0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1968

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			behavior through a format string injection vulnerability in a web interface API.					
			CVE ID : CVE-2023- 25492					
Product: thi	inkagile_hx3331	_firmwaı	е	<u> </u>				
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1969			
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1970			
Affected Ver	Affected Version(s): * Up to (excluding) 4.71_d8bt48p							
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1971			

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/1972
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx3375	_firmwai	re		
Affected Ver	sion(s): * Up to (e	excluding)	4.71_d8bt48p		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1973
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1974

0-1

1-2

**2-3** 3-4 4-5 Page **855** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Product: th	inkagile_hx3376	5_firmwa1	re	I	L	
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1975	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b> 25492	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/1976	
Due du et th		a Garage	25492			
	inkagile_hx3520					
Affected Ver	sion(s): * Up to (e	excluding)				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1977	
Use of Externally- Controlled	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC	https://supp ort.lenovo.co m/us/en/pr oduct_securi	O-LEN-THIN- 170523/1978	
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10						

Format String			web user interface or	ty/LEN-	
			other undefined behavior through a format string injection vulnerability in a web interface API.	99936	
			CVE ID : CVE-2023- 25492		
Product: thi	nkagile_hx3521	-g_firmw	are		
Affected Vers	sion(s): * Up to (e	excluding)	3.72_tei388s		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1979
			CVE ID : CVE-2023- 0683	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1980
			CVE ID : CVE-2023- 25492		
	nkagile_hx3720				
Affected Vers	sion(s): * Up to (e	excluding)			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi	O-LEN-THIN- 170523/1981
CVSS Scoring S	Scale 0-1 1	-2 2-3	3-4 4-5 5-6 Page <b>857</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.	ty/LEN- 99936	
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1982
			CVE ID : CVE-2023- 25492		
	inkagile_hx3721				
Affected Ver	sion(s): * Up to (e	excluding)			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/1983
			CVE ID : CVE-2023- 0683	77730	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1984

0-1

1-2

**2-3** 3-4 4-5 Page **858** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx552(	)-c_firmw	are		
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1985
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1986
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx552(	)_firmwai	re		
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1987
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	O-LEN-THIN- 170523/1988

0-1

1-2

**2-3** 3-4 4-5 Page **859** of **1106**  6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936	
Product: thi	nkagile_hx5521	-c_firmw	are		
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1989
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1990
			25492		
	nkagile_hx5521				
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a		

0-1

1-2

**2-3** 3-4 4-5 Page **860** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/1991
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1992
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx5530	)_firmwai	re		
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/1993
			0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1994

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			behavior through a format string injection vulnerability in a web interface API.					
			CVE ID : CVE-2023- 25492					
Product: thi	inkagile_hx5531	_firmwaı	re	L				
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1995			
			CVE ID : CVE-2023- 0683					
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/1996			
			CVE ID : CVE-2023- 25492					
	Product: thinkagile_hx7520_firmware							
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1997			

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1998
			CVE ID : CVE-2023- 25492		
	inkagile_hx7521				
Affected Ver	sion(s): * Up to (e	excluding)	<u>^</u>	1	
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/1999
			CVE ID : CVE-2023- 0683	<i>,,,,</i> ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2000

0-1

1-2

**2-3** 3-4 4-5 Page **863** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx7530	_firmwai	re		
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2001
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2002
			25492		
Product: th	inkagile_hx7531	_firmwai	re		
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2003
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	O-LEN-THIN- 170523/2004

0-1

1-2

**2-3** 3-4 4-5 Page **864** of **1106**  6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936				
Affected Ver	sion(s): * Up to (e	excluding)	2.75_psi348s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2005			
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2006			
	Product: thinkagile_hx7820_firmware							
Affected Ver	sion(s): * Up to (e	excluding)	-	latter c //				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only	https://supp ort.lenovo.co m/us/en/pr	0-LEN-THIN- 170523/2007			
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10           Page 865 of 1106								

Page 865 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access may gain elevated privileges through a specifically crafted API call.	oduct_securi ty/LEN- 99936	
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2008
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx7821	_firmwaı	'e		
Affected Ver	sion(s): * Up to (e	excluding)	3.72_tei388s		
N/A	01-May-2023	01-May-2023 8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2009
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2010

0-1

1-2

**2-3** 3-4 4-5 Page **866** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in a web interface API.		
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_hx_encl	osure_fir	mware		
Affected Ver	sion(s): * Up to (e	excluding)	3.72_tei388s		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2011
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2012
Product: thi	inkagile_mx102	) firmwa	25492		
	sion(s): * Up to (e				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023- 0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2013

0-1

1-2

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2014		
			CVE ID : CVE-2023- 25492				
Product: thi	inkagile_mx102	1_on_se3					
Affected Ver	sion(s): * Up to (	excluding)	) 3.72_tei388s				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023- 0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2015		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2016		
		0.6.6	CVE ID : CVE-2023- 25492				
Product: thinkagile_mx3330-f_firmware Affected Version(s): * Up to (excluding) 2.93_afbt30p							
Anecteu version(s): Op to (excluding) 2.95_abitsop							
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3 3-4 4-5 5-6</b> Page <b>868</b> of <b>1106</b>	6-7 7-8	3 8-9 <mark>9-10</mark>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2017
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2018
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_mx333	0-h_firmv	vare		
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p	-	
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2019
			0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2020

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inkagile_mx333	1-f_firmw	are	<u> </u>			
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2021		
			CVE ID : CVE-2023- 0683				
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2022		
			CVE ID : CVE-2023- 25492				
Product: thinkagile_mx3331-h_firmware							
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p	1			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2023		

 CVSS Scoring Scale
 0-1
 1-2
 2-3
 3-4

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2024
			CVE ID : CVE-2023- 25492		
	inkagile_mx353				
Affected Ver	sion(s): * Up to (e	excluding)	<b>^</b>		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2025
			CVE ID : CVE-2023- 0683	99930	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2026

0-1

1-2

2-33-44-5Page 871 of 1106

5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: th	inkagile_mx353	0_f_firmw	are		
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2027
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2028
			25492		
	inkagile_mx353				
Affected Ver	sion(s): * Up to (e	excluding)			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2029
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	O-LEN-THIN- 170523/2030

0-1

1-2

2-33-44-5Page 872 of 1106

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936		
Product: thi	inkagile_mx353	1_h_firmv	vare			
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2031	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2032	
			CVE ID : CVE-2023- 25492			
Product: thi	inkagile_vx1320	_firmwar	'e		·	
Affected Version(s): * Up to (excluding) 3.72_tei388s						

0-1

1-2

**2-3** 3-4 4-5 Page **873** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2033
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2034
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_vx2320	_firmwar	е		
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2035
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2036

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inkagile_vx2330	_firmwar	e	L			
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2037		
			CVE ID : CVE-2023- 0683	77730			
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2038		
			CVE ID : CVE-2023- 25492				
Product: thinkagile_vx3320_firmware							
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2039		

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2040
			CVE ID : CVE-2023- 25492		
	inkagile_vx3330				
Affected Ver	sion(s): * Up to (e	excluding)	<b>^</b>		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2041
			CVE ID : CVE-2023- 0683	<i></i>	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2042

0-1

1-2

**2-3** 3-4 4-5 Page **876** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_vx3331	_firmwaı	.e		
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2043
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2044
			25492		
Product: thi	inkagile_vx3520	-g_firmw	are		
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2045
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	0-LEN-THIN- 170523/2046

0-1

1-2

**2-3** 3-4 4-5 Page **877** of **1106**  6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936			
Product: thi	inkagile_vx3530	-g_firmw	are	<u> </u>			
Affected Vers	sion(s): * Up to (e	excluding)	2.93_afbt30p				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2047		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2048		
			CVE ID : CVE-2023- 25492				
Product: thi	inkagile_vx3720	_firmwar	е		·		
Affected Version(s): * Up to (excluding) 3.72_tei388s							

0-1

1-2

**2-3** 3-4 4-5 Page **878** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2049
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2050
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_vx5520	_firmwar	е		
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2051
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2052

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			behavior through a format string injection vulnerability in a web interface API.					
			CVE ID : CVE-2023- 25492					
Product: thi	inkagile_vx5530	_firmwar	е					
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p					
N/A	01-May-2023	•May-2023 8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2053			
			CVE ID : CVE-2023- 0683	79930				
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2054			
			CVE ID : CVE-2023- 25492					
	Product: thinkagile_vx7320_n_firmware							
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2055			

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2056
			CVE ID : CVE-2023- 25492		
	inkagile_vx7330				
Affected Ver	sion(s): * Up to (e	excluding)	<b>^</b>	1	
N/A	01-May-2023	01-May-2023 8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2057
			CVE ID : CVE-2023- 0683	<i>,,,,</i> ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2058

0-1

1-2

**2-3** 3-4 4-5 Page **881** of **1106**  5-6

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_vx7520	_firmwaı	'e		
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2059
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2060
			25492		
Product: thi	inkagile_vx7520	_n_firmw	are		
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2061
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	O-LEN-THIN- 170523/2062

0-1

1-2

**2-3** 3-4 4-5 Page **882** of **1106**  6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936			
Product: thi	nkagile_vx7530	_firmwar	е				
Affected Vers	sion(s): * Up to (e	excluding)	2.93_afbt30p				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2063		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2064		
			25492				
Product: thi	nkagile_vx7531	_firmwar	е				
Affected Version(s): * Up to (excluding) 2.93_afbt30p							

0-1

1-2

**2-3** 3-4 4-5 Page **883** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2065
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2066
			CVE ID : CVE-2023- 25492		
Product: thi	inkagile_vx7820	_firmwar	'e		
Affected Ver	sion(s): * Up to (e	excluding)	2.75_psi348s		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2067
			0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2068

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inkagile_vx_1se_	firmware	9	L			
Affected Ver	sion(s): * Up to (e	excluding)	3.72_tei388s				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2069		
			CVE ID : CVE-2023- 0683	77730			
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2070		
			CVE ID : CVE-2023- 25492				
	inkagile_vx_2u4						
Affected Version(s): * Up to (excluding) 3.72_tei388s							
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2071		

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2072
			CVE ID : CVE-2023- 25492		
	nkagile_vx_4u_f				
Affected Ver	sion(s): * Up to (e	excluding)	*		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2073
			CVE ID : CVE-2023- 0683	<i></i>	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2074

0-1

1-2

**2-3** 3-4 4-5 Page **886** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: th	inkedge_se450_	firmwar	e		
Affected Ver	sion(s): * Up to (e	excluding)	1.60_usx324o		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2075
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2076
			25492		
	inkstation_p920				
Affected Ver	sion(s): * Up to (e	excluding)			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2077
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	O-LEN-THIN- 170523/2078

0-1

1-2

**2-3** 3-4 4-5 Page **887** of **1106**  6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936	
Product: thi	inksystem_sd53	0_firmwa	re		
Affected Ver	sion(s): * Up to (e	excluding)	3.72_tei388s		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2079
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2080
			25492		
	inksystem_sd63				
Affected Ver	sion(s): * Up to (e	excluding)	2.60_tgbt42h		

0-1

1-2

**2-3** 3-4 4-5 Page **888** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2081
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2082
			CVE ID : CVE-2023- 25492		
Product: thi	inksystem_sd65	0-n_v2_fi	rmware		
Affected Ver	sion(s): * Up to (e	excluding)	2.60_tgbt42h		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2083
			0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2084

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inksystem_sd65	0_firmwa	re				
Affected Ver	sion(s): * Up to (e	excluding)	3.72_tei388s				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2085		
			CVE ID : CVE-2023- 0683	55530			
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2086		
			CVE ID : CVE-2023- 25492				
Product: thinksystem_sd650_v2_firmware							
Affected Ver	sion(s): * Up to (e	excluding)	2.60_tgbt42h				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2087		

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2088
			CVE ID : CVE-2023- 25492		
	inksystem_se35				
Affected Ver	sion(s): * Up to (e	excluding)			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2089
			CVE ID : CVE-2023- 0683	77750	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2090

0-1

1-2

**2-3** 3-4 4-5 Page **891** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inksystem_sn55	0_firmwa	re		
Affected Ver	sion(s): * Up to (	excluding)	3.72_tei388s		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2091
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2092
			25492		
Product: thi	inksystem_sn55	0_v2_firm	iware		<u> </u>
Affected Ver	sion(s): * Up to (	excluding)	2.60_tgbt42h		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2093
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	O-LEN-THIN- 170523/2094

0-1

1-2

**2-3** 3-4 4-5 Page **892** of **1106**  6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936				
Product: thi	inksystem_sn85	0_firmwa	re	<u> </u>				
Affected Ver	sion(s): * Up to (e	excluding)	3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2095			
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2096			
<b>D</b>			25492					
	Product: thinksystem_sr150_firmware							
Affected Version(s): * Up to (excluding) 3.72_tei388s								

0-1

1-2

**2-3** 3-4 4-5 Page **893** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2097
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2098
			CVE ID : CVE-2023- 25492		
Product: thi	inksystem_sr15	8_firmwa	re		
Affected Ver	sion(s): * Up to (e	excluding)	3.72_tei388s		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2099
			0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2100

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inksystem_sr25	0_firmwa	re	<u> </u>			
Affected Ver	sion(s): * Up to (e	excluding)	3.72_tei388s				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2101		
			CVE ID : CVE-2023- 0683	79930			
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2102		
			CVE ID : CVE-2023- 25492				
Product: thinksystem_sr250_v2_firmware							
Affected Ver	sion(s): * Up to (e	excluding)	2.60_tgbt42h				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2103		

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2104
			CVE ID : CVE-2023- 25492		
	inksystem_sr25				
Affected Ver	sion(s): * Up to (e	excluding)			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2105
			CVE ID : CVE-2023- 0683	<i></i>	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2106

0-1

1-2

**2-3** 3-4 4-5 Page **896** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inksystem_sr25	8_v2_firm	ware		
Affected Ver	sion(s): * Up to (e	excluding)	2.60_tgbt42h		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2107
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2108
			25492		
	inksystem_sr53				
Affected Ver	sion(s): * Up to (e	excluding)			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2109
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	O-LEN-THIN- 170523/2110

0-1

1-2

**2-3** 3-4 4-5 Page **897** of **1106**  6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936		
Product: thi	inksystem_sr55	0_firmwa	re			
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2111	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2112	
<b>D</b>			25492			
	inksystem_sr57					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a						

0-1

1-2

**2-3** 3-4 4-5 Page **898** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2113
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2114
			CVE ID : CVE-2023- 25492		
Product: thi	inksystem_sr59	0_firmwa	re		
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2115
			0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2116

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			behavior through a format string injection vulnerability in a web interface API.				
			CVE ID : CVE-2023- 25492				
Product: thi	inksystem_sr63	0_firmwa	re				
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2117		
			CVE ID : CVE-2023- 0683	55530			
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2118		
			CVE ID : CVE-2023- 25492				
Product: thinksystem_sr630_v2_firmware							
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2119		

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2120
			CVE ID : CVE-2023- 25492		
	inksystem_sr64				
Affected Ver	sion(s): * Up to (e	excluding)	•		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2121
			CVE ID : CVE-2023- 0683	<i></i>	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2122

0-1

1-2

**2-3** 3-4 4-5 Page **901** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inksystem_sr64	5_v3_firm	ware		
Affected Ver	sion(s): * Up to (e	excluding)	4.71_d8bt48p		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2123
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2124
			25492		
Product: thi	inksystem_sr65	0_firmwa	re		
Affected Ver	sion(s): * Up to (e	excluding)	8.88_cdi3a4a		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2125
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	O-LEN-THIN- 170523/2126

0-1

1-2

**2-3 3-4 4-5** Page **902** of **1106**  6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936	
Product: thi	nksystem_sr65	)_v2_firm	ware	<u> </u>	<u> </u>
Affected Ver	sion(s): * Up to (e	excluding)	2.93_afbt30p		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2127
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2128
			CVE ID : CVE-2023- 25492		
	nksystem_sr66				
Affected Ver	sion(s): * Up to (e	excluding)	4.71_d8bt48p		

0-1

1-2

**2-3** 3-4 4-5 Page **903** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2129
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2130
			CVE ID : CVE-2023- 25492		
Product: thi	inksystem_sr66	5_v3_firm	ware		
Affected Ver	sion(s): * Up to (e	excluding)	4.71_d8bt48p		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2131
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2132

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			behavior through a format string injection vulnerability in a web interface API.					
			CVE ID : CVE-2023- 25492					
Product: thi	inksystem_sr67	0_firmwa	re					
Affected Ver	sion(s): * Up to (e	excluding)	3.72_tei388s					
N/A	01-May-2023	1ay-2023 8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2133			
			CVE ID : CVE-2023- 0683	99930				
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2134			
			CVE ID : CVE-2023- 25492					
	Product: thinksystem_sr670_v2_firmware							
Affected Ver	sion(s): * Up to (e	excluding)	2.60_tgbt42h					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2135			

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2136
			CVE ID : CVE-2023- 25492		
	inksystem_sr85				
Affected Ver	sion(s): * Up to (e	excluding)			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2137
			CVE ID : CVE-2023- 0683	<i>,,,,</i> ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2138

0-1

1-2

**2-3** 3-4 4-5 Page **906** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inksystem_sr85	0_firmwa	re		
Affected Ver	sion(s): * Up to (e	excluding)	3.72_tei388s		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2139
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2140
			25492		
Product: thi	inksystem_sr85	0_v2_firm	ware		I
Affected Ver	sion(s): * Up to (e	excluding)	2.60_tgbt42h		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2141
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	O-LEN-THIN- 170523/2142

0-1

1-2

**2-3** 3-4 4-5 Page **907** of **1106**  6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID						
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b> <b>25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936							
Product: thi	inksystem_sr86	0_firmwa	re		<u> </u>						
Affected Ver	sion(s): * Up to (e	excluding)	3.72_tei388s								
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. CVE ID : CVE-2023- 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2143						
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2144						
<b>D</b> 1			25492								
	inksystem_sr86										
Affected Ver	sion(s): * Up to (e	excluding)	2.60_tgbt42h		Affected Version(s): * Up to (excluding) 2.60_tgbt42h						

0-1

1-2

**2-3** 3-4 4-5 Page **908** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2145
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2146
			CVE ID : CVE-2023- 25492		
Product: thi	inksystem_sr95	0_firmwa	re		
Affected Ver	sion(s): * Up to (e	excluding)	2.75_psi348s		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2147
			0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2148

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			behavior through a format string injection vulnerability in a web interface API.					
			CVE ID : CVE-2023- 25492					
Product: thi	inksystem_st25(	)_firmwa	re	<u> </u>				
Affected Ver	sion(s): * Up to (e	excluding)	3.72_tei388s					
N/A	01-May-2023	-May-2023 8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2149			
			CVE ID : CVE-2023- 0683	99930				
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2150			
			CVE ID : CVE-2023- 25492					
	Product: thinksystem_st250_v2_firmware							
Affected Ver	sion(s): * Up to (e	excluding)	2.60_tgbt42h					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2151			

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call.		
			CVE ID : CVE-2023- 0683		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2152
			CVE ID : CVE-2023- 25492		
	inksystem_st258				
Affected Ver	sion(s): * Up to (e	excluding)			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2153
			CVE ID : CVE-2023- 0683	57530	
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2154

0-1

1-2

2-33-44-5Page 911 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 25492		
Product: thi	inksystem_st25	8_v2_firm	ware		
Affected Ver	sion(s): * Up to (e	excluding)	2.60_tgbt42h		
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2155
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2156
			25492		
	inksystem_st55				
Affected Ver	sion(s): * Up to (e	excluding)			
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> 0683	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	O-LEN-THIN- 170523/2157
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://supp ort.lenovo.co	0-LEN-THIN- 170523/2158

0-1

1-2

2-33-44-5Page 912 of 1106

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023- 25492</b>	m/us/en/pr oduct_securi ty/LEN- 99936			
Product: thi	inksystem_st65(	)_v2_firm	ware	<u> </u>	<u> </u>		
Affected Ver	sion(s): * Up to (e	excluding)	2.60_tgbt42h				
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b> <b>0683</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2159		
Use of Externally- Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	https://supp ort.lenovo.co m/us/en/pr oduct_securi ty/LEN- 99936	0-LEN-THIN- 170523/2160		
			25492				
Product: thinksystem_st658_v2_firmware							
Affected Ver	Affected Version(s): * Up to (excluding) 2.60_tgbt42h						

0-1

1-2

2-33-44-5Page 913 of 1106

5-6

6-7

7-8 8-9

N/A01-May-20238.8A valid, authenticated XCC user with read only access may gain elevated privileges (rafted API call. CVE ID : CVE-2023- 0683https://supp oduct.securi ty/LEN- 99360-LEN-THIN- 170523/2161Use of Externally- Controlled Format String01-May-20238.8A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. CVE ID : CVE-2023- 25492https://supp oduct.securi ty/LEN- 99360-LEN-THIN- 170523/2162Vendor: LinuxAn issue was discovered in the Linux kernel Before 6.1.11. Im net/netrom/af.netro after-free because after-free because after-free because after-free because after-free because after-free because after-free because ascressfully connected AF,NETROM socket. However, in order for an attacker to explored before ascressfully connected AF,NETROM socket. However, in order for an attacker to explored before ascressfully connected action this, the explored before ascressfully connected action this, the system must havehttps://githu doit.0-LIN-LINU- 170523/2163VUSS Storing Scale01 101010101010VISS Storing Scale <t< th=""><th>Weakness</th><th>Publish Date</th><th>CVSSv3</th><th>Description &amp; CVE ID</th><th>Patch</th><th>NCIIPC ID</th></t<>	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Use of Externally Controlled Format String01-May-20238.8authenticated user may be able to trigger a denial of service of the XCC other undefined behavior through a format string injection vulnerability in a web interface API. CYE ID : CVE-2023- 25492https://supp oduct_securi ty/LEN- 99360-LEN-THIN- 170523/2162Vendor: Linux FreeVendor: Linux service of the XCC other undefined behavior through a or through a service of the XCC vulnerability in a web interface API. CYE ID : CVE-2023- 25492https://supp oduct_securi ty/LEN- 99360-LEN-THIN- 170523/2162Vendor: Linux FreeVendor: Linux service of the XCC vulnerability in a web interface API. Linux kernel before 6.1.11.https://githu b.com/torval ds/linux/co mmit/61179 2920925/b0 88ddcobe27 83c7/92/dth0-LIN-LINU- 170523/2163Use After Free05-May-20236.7An issue was discovered in the Linux kernel before 6.1.11. In net/netrom/af_netro m.c. there is a use- after-free because accept is also allowed for a successfully connected AF_NETROM socket. However, in order for an attacker to exploit this, the system must have0-LIN-LINU- 170523/2163	N/A	01-May-2023	8.8	authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. <b>CVE ID : CVE-2023-</b>	ort.lenovo.co m/us/en/pr oduct_securi ty/LEN-			
Product: linux_kernel         Affected Version(s): * Up to (excluding) 6.1.11         An issue was         discovered in the         Linux kernel before         6.1.11. In         net/netrom/af_netro         m.c, there is a use-         after-free because         discovered in the         use After         Free         05-May-2023         6.7         An issue was         after-free because         after-free because         after-free because         allowed for a         successfully         connected         AF_NETROM socket.         However, in order         for an attacker to         exploit this, the         system must have	Externally- Controlled Format	01-May-2023	8.8	authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. <b>CVE ID : CVE-2023-</b>	ort.lenovo.co m/us/en/pr oduct_securi ty/LEN-			
Affected Version(s): * Up to (excluding) 6.1.11Affected Version(s): * Up to (excluding) 6.1.11An issue was discovered in the Linux kernel before 6.1.11. In net/netrom/af_netro m.c, there is a use- after-free because after-free because allowed for a successfully connected AF_NETROM socket. However, in order for an attacker to exploit this, the system must have	Vendor: Lin	ux			I			
Use After Free05-May-20236.7An issue was discovered in the Linux kernel before 6.1.11. In net/netrom/af_netro m.c, there is a use- after-free because allowed for a successfully connected AF_NETROM socket. However, in order for an attacker to exploit this, the system must havehttps://githu b.com/torval ds/linux/co mmit/61179 0-LIN-LINU- 170523/2163	Product: lin	ux_kernel						
Use After Free05-May-20236.7discovered in the Linux kernel before 6.1.11. In net/netrom/af_netro inc, there is a use- after-free becausehttps://githu b.com/torval ds/linux/co accept is also0-LIN-LINU- 170523/2163Free05-May-20236.7accept is also allowed for a allowed for ammit/61179 2920925fb00-LIN-LINU- 170523/2163AF_NETROM socket.6b64444However, in order for an attacker to system must have6b644	Affected Ver	sion(s): * Up to (e	excluding)	6.1.11				
	Use After Free05-May-20236.7discovered in the Linux kernel before 6.1.11. In net/netrom/af_netro m.c, there is a use- after-free becausehttps://githu b.com/torval ds/linux/co ads/linux/co 2920925fb00-LIN-LINU- 170523/2163See After Free6.76.788ddccbe27 connected AF_NETROM socket. However, in order for an attacker to exploit this, the88ddccbe27 bed0-LIN-LINU- 170523/2163							

Page **914** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netrom routing configured or the attacker must have the CAP_NET_ADMIN capability.		
			CVE ID : CVE-2023- 32269		
Affected Ver	sion(s): * Up to (i	ncluding)	5.19	L	<u> </u>
Use After Free	08-May-2023	6.7	A use-after-free vulnerability was found in the Linux kernel's ext4 filesystem in the way it handled the extra inode size for extended attributes. This flaw could allow a privileged local user to cause a system crash or other undefined behaviors. <b>CVE ID : CVE-2023-</b> <b>2513</b>	https://githu b.com/torval ds/linux/co mmit/67d7d 8ad99be	0-LIN-LINU- 170523/2164
Affected Ver	sion(s): * Up to (i	ncluding)	6.3.1		
Use After Free	08-May-2023	7.8	In the Linux kernel through 6.3.1, a use- after-free in Netfilter nf_tables when processing batch requests can be abused to perform arbitrary read and write operations on kernel memory. Unprivileged local users can obtain root privileges. This occurs because anonymous sets are mishandled.	https://githu b.com/torval ds/linux/co mmit/c1592 a89942e967 8f7d9c8030e fa777c0d57e dab, https://git.k ernel.org/cgi t/linux/kern el/git/torval ds/linux.git/ commit/?id= c1592a8994 2e9678f7d9c	O-LIN-LINU- 170523/2165

0-1

1-2

2-33-44-5Page 915 of 1106

5-6

6-7

7-8 8-9

Image: here of the second se	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free01-May-20237.8A use-after-free vulnerability in the Linux Kernel io_uring subsystem can be exploited to achieve local privilege escalation.https://kern el.dance/9d9 4c04c0db02 4922e886c9fd 429659c9f 48ea4, https://git.k ernel.org/pu0-LIN-LINU- 170523/2166Use After Free01-May-20237.8A use-after-free vulnerability.https://git.k ernel.git/t orvalds/linu x.git/commit /?id=904c0 40040b02492 2e886c9fd429659f20-LIN-LINU- 170523/2166Use After Free01-May-20237.8A use-after-free vulnerability.https://kern el.dance/409 4004b02492 2e886c9fd429659f20-LIN-LINU- 170523/2166Mice After Free01-May-20237.8A use-after-free vulnerability in the Linux Kernel Performance Events system can be exploited to achieve eladation.https://kern eladacc/fid 943edccc7fd e947a2, https://git.k ernel.org/pu0-LIN-LINU- 170523/2167						
Use After Free01-May-20237.8A use-after-free vulnerability in the Linux Kernel io_uring subsystem can be exploited to achieve local privilege escalation.https://kern el.dance/9d9 402040b02 4022e886c9f d429659f22f 48ea4, https://git.k ernel.org/pu b/scm/linux /kernel/git/t orvalds/linux /kernel/git/t orvalds/linux /kernel/git/t orvalds/linux /kernel/git/t orvalds/linux /kernel/git/t orvalds/linux /kernel/git/t orvalds/linux /kernel/git/t orvalds/linux /kernel/git/t orvalds/linux /kernel/git/t orvalds/linux kernel-org/pu b/scm/linux /kernel/git/t orvalds/linux kernel-org/pu b/scm/linux /kernel/git/t orvalds/linux kernel-org/pu b/scm/linux /kernel/git/t orvalds/linux kernel-org/pu b/scm/linux kernel-org/pu b/scm/linux kernel-org/pu b/scm/linux kernel-org/pu b/scm/linux kernel-org/pu b/scm/linux kernel-org/pu b/scm/linux kernel-org/pu b/scm/linux kernel-org/pu b/scm/linux kernel-org/pu ad40-LIN-LINU- 170523/21664ffected Versor(s): 6.364400 commit orvalds/linu kernel berformance Events system can be exploited to achieve local privilege escalation.https://kern el.dance/fd0 el.1N-LINU- 170523/2167	Affected Ver	sion(s): 6.1			<u> </u>	
Affected Version(s): 6.3A use-after-free vulnerability in the Linux Kernel Performance Events system can be exploited to achieve local privilege escalation.https://kern el.dance/fd0 815f632c24 878e325821 943edccc7fd e947a2, https://git.k ernel.org/puO-LIN-LINU- 170523/2167		01-May-2023	7.8	<ul> <li>vulnerability in the Linux Kernel</li> <li>io_uring subsystem</li> <li>can be exploited to</li> <li>achieve local</li> <li>privilege escalation.</li> </ul> Both io_install_fixed_ file and its callers call fput in a file in case of an error, causing a reference <ul> <li>underflow which</li> <li>leads to a use-after-</li> <li>free vulnerability.</li> </ul> We recommend <ul> <li>upgrading past</li> <li>commit</li> <li>9d94c04c0db02492</li> <li>2e886c9fd429659f2</li> <li>2f48ea4.</li> </ul>	el.dance/9d9 4c04c0db02 4922e886c9f d429659f22f 48ea4, https://git.k ernel.org/pu b/scm/linux /kernel/git/t orvalds/linu x.git/commit /?id=9d94c0 4c0db02492 2e886c9fd42 9659f22f48e	0-LIN-LINU- 170523/2166
Use After Free 01-May-2023 7.8 A use-after-free vulnerability in the el.dance/fd0 5.2 Performance Events system can be exploited to achieve local privilege escalation. 4.2 Particular to achieve escalation. 4.2 Performance Events be exploited to achieve enel.org/pu based of the privilege erel.org/pu based of the privilege erel.org				2236		
Use After Free 01-May-2023 7.8 7.8 7.8 7.8 7.8 7.8 7.8 7.8 7.8 7.8	Affected Ver	sion(s): 6.3				
		01-May-2023	7.8	vulnerability in the Linux Kernel Performance Events system can be exploited to achieve local privilege	el.dance/fd0 815f632c24 878e325821 943edccc7fd e947a2, https://git.k	0-LIN-LINU- 170523/2167
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	Scale 0-1	1-2 2-3	3-4 4-5 5-6	6-7 7.9	8 8-9 9-10

2-3 Page **916** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The perf_group_detach function did not check the event's siblings' attach_state before calling add_event_to_groups (), but remove_on_exec made it possible to call list_del_event() on before detaching from their group, making it possible to use a dangling pointer causing a use-after-free vulnerability. We recommend upgrading past commit fd0815f632c24878e 325821943edccc7fd e947a2.	/kernel/git/t orvalds/linu x.git/commit /?id=fd0815f 632c24878e 325821943e dccc7fde947 a2	
			CVE ID : CVE-2023- 2235		
Affected Ver	sion(s): From (in	cluding) 5	.13 Up to (excluding) 6.	3	
Use After Free	01-May-2023	7.8	A use-after-free vulnerability in the Linux Kernel Performance Events system can be exploited to achieve local privilege escalation. The perf_group_detach	https://kern el.dance/fd0 815f632c24 878e325821 943edccc7fd e947a2, https://git.k ernel.org/pu b/scm/linux /kernel/git/t orvalds/linu x.git/commit	O-LIN-LINU- 170523/2168
CVSS Searing		1 2 2 2		67 70	
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10           Page 917 of 1106					

Page **917** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function did not check the event's siblings' attach_state before calling add_event_to_groups (), but remove_on_exec made it possible to call list_del_event() on before detaching from their group, making it possible to use a dangling pointer causing a use-after-free vulnerability.	/?id=fd0815f 632c24878e 325821943e dccc7fde947 a2	
			We recommend upgrading past commit fd0815f632c24878e 325821943edccc7fd e947a2. <b>CVE ID : CVE-2023-</b>		
			2235		
Affected Ver	sion(s): From (in	cluding) 5	.19 Up to (excluding) 6.	1	
Use After Free	01-May-2023	7.8	A use-after-free vulnerability in the Linux Kernel io_uring subsystem can be exploited to achieve local privilege escalation. Both io_install_fixed_ file and its callers call fput in a file in case of an error, causing a reference	https://kern el.dance/9d9 4c04c0db02 4922e886c9f d429659f22f 48ea4, https://git.k ernel.org/pu b/scm/linux /kernel/git/t orvalds/linu x.git/commit /?id=9d94c0 4c0db02492	0-LIN-LINU- 170523/2169
CVSS Scoring S	Scale 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>
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10           Page 918 of 1106					

Page **918** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underflow which leads to a use-after- free vulnerability.	2e886c9fd42 9659f22f48e a4	
			We recommend upgrading past commit 9d94c04c0db02492 2e886c9fd429659f2 2f48ea4.		
			CVE ID : CVE-2023- 2236		
Vendor: Mic					
Affected Ver					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-May-2023	9.8	CLTPHP <=6.0 is vulnerable to Improper Input Validation. CVE ID : CVE-2023- 30268	N/A	O-MIC-WIND- 170523/2170
Improper Enforceme nt of Message Integrity During Transmissi on in a Communic ation Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f 5.com/mana ge/s/article/ K000132522	0-MIC-WIND- 170523/2171

0-1

1-2

**2-3** 3-4 4-5 Page **919** of **1106**  5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 22372		
Improper Certificate Validation	03-May-2023	5.9	An improper certificate validation vulnerabil ity exists in the BIG- IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. <b>CVE ID : CVE-2023- 24461</b>	https://my.f 5.com/mana ge/s/article/ K000132539	O-MIC-WIND- 170523/2172
Product: wi	ndows_10_1507	,			
Affected Ver	sion(s): * Up to (e	excluding)	10.0.10240.19926		
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24943	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24943	0-MIC-WIND- 170523/2173
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24903	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24903	O-MIC-WIND- 170523/2174

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability <b>CVE ID : CVE-2023- 28283</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28283	O-MIC-WIND- 170523/2175
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24946	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24946	O-MIC-WIND- 170523/2176
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability CVE ID : CVE-2023- 24901	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24901	O-MIC-WIND- 170523/2177
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability CVE ID : CVE-2023- 24939	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24939	O-MIC-WIND- 170523/2178
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability <b>CVE ID : CVE-2023-</b> <b>24940</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24940	O-MIC-WIND- 170523/2179
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability CVE ID : CVE-2023- 24942	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24942	O-MIC-WIND- 170523/2180

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability CVE ID : CVE-2023- 29325	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29325	O-MIC-WIND- 170523/2181
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	O-MIC-WIND- 170523/2182
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24948	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24948	O-MIC-WIND- 170523/2183
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability CVE ID : CVE-2023- 24932	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24932	O-MIC-WIND- 170523/2184
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29324	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29324	O-MIC-WIND- 170523/2185
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability CVE ID : CVE-2023- 24900	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24900	0-MIC-WIND- 170523/2186
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2187

0-1

1-2

2-33-44-5Page 922 of 1106

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability	ability/CVE- 2023-24945	
			CVE ID : CVE-2023- 24945		
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability <b>CVE ID : CVE-2023-</b> <b>28251</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28251	O-MIC-WIND- 170523/2188
Product: wi	ndows_10_1607	,			
Affected Ver	sion(s): * Up to (e	excluding)	10.0.14393.5921		
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24943	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24943	O-MIC-WIND- 170523/2189
N/A	09-May-2023	8.8	Windows Bluetooth Driver Remote Code Execution Vulnerability CVE ID : CVE-2023- 24947	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24947	O-MIC-WIND- 170523/2190
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24903	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24903	0-MIC-WIND- 170523/2191
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP)	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2192

0-1

1-2

2-33-44-5Page 923 of 1106

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability	ability/CVE- 2023-28283	
			CVE ID : CVE-2023- 28283		
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24946	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24946	O-MIC-WIND- 170523/2193
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability CVE ID : CVE-2023- 24901	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24901	0-MIC-WIND- 170523/2194
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability CVE ID : CVE-2023- 24939	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24939	O-MIC-WIND- 170523/2195
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability <b>CVE ID : CVE-2023-</b> <b>24940</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24940	O-MIC-WIND- 170523/2196
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability CVE ID : CVE-2023- 24942	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24942	O-MIC-WIND- 170523/2197
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2198

0-1

1-2

**2-3** 3-4 4-5 Page **924** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29325	ability/CVE- 2023-29325	
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	0-MIC-WIND- 170523/2199
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24948	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24948	O-MIC-WIND- 170523/2200
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability CVE ID : CVE-2023- 24932	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24932	0-MIC-WIND- 170523/2201
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29324	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29324	O-MIC-WIND- 170523/2202
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability CVE ID : CVE-2023- 24900	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24900	0-MIC-WIND- 170523/2203
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability CVE ID : CVE-2023- 24945	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24945	0-MIC-WIND- 170523/2204

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability CVE ID : CVE-2023- 28251	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28251	O-MIC-WIND- 170523/2205
Product: wi	ndows_10_1809	)			<u> </u>
Affected Ver	sion(s): * Up to (e	excluding)	10.0.17763.4377		
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24943	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24943	0-MIC-WIND- 170523/2206
N/A	09-May-2023	8.8	Windows Bluetooth Driver Remote Code Execution Vulnerability CVE ID : CVE-2023- 24947	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24947	O-MIC-WIND- 170523/2207
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24903	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24903	0-MIC-WIND- 170523/2208
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28283	O-MIC-WIND- 170523/2209

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 28283		
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24946	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24946	O-MIC-WIND- 170523/2210
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24949	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24949	O-MIC-WIND- 170523/2211
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability CVE ID : CVE-2023- 24901	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24901	O-MIC-WIND- 170523/2212
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability CVE ID : CVE-2023- 24939	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24939	O-MIC-WIND- 170523/2213
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability <b>CVE ID : CVE-2023-</b> <b>24940</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24940	O-MIC-WIND- 170523/2214
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability CVE ID : CVE-2023- 24942	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24942	O-MIC-WIND- 170523/2215

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability CVE ID : CVE-2023- 29325	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29325	O-MIC-WIND- 170523/2216
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	O-MIC-WIND- 170523/2217
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24948	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24948	O-MIC-WIND- 170523/2218
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability CVE ID : CVE-2023- 24932	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24932	O-MIC-WIND- 170523/2219
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information Disclosure Vulnerability CVE ID : CVE-2023- 24944	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24944	O-MIC-WIND- 170523/2220
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29324	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29324	O-MIC-WIND- 170523/2221
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2222

0-1

1-2

**2-3** 3-4 4-5 Page **928** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability	ability/CVE- 2023-24900	
			CVE ID : CVE-2023- 24900		
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability CVE ID : CVE-2023- 24945	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24945	O-MIC-WIND- 170523/2223
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability CVE ID : CVE-2023- 28251	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28251	O-MIC-WIND- 170523/2224
Product: wi	ndows_10_20h2				
Affected Ver	sion(s): * Up to (e	excluding)	10.0.19042.2965		
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24943	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24943	O-MIC-WIND- 170523/2225
N/A	09-May-2023	8.8	Windows Bluetooth Driver Remote Code Execution Vulnerability CVE ID : CVE-2023- 24947	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24947	O-MIC-WIND- 170523/2226
Concurrent Execution using Shared Resource with Improper Synchroniz	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24903	O-MIC-WIND- 170523/2227

0-1

1-2

**2-3** 3-4 4-5 Page **929** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
ation ('Race Condition')			CVE ID : CVE-2023- 24903				
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 28283	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28283	O-MIC-WIND- 170523/2228		
N/A	09-May-2023	7.8	Remote Desktop Client Remote Code Execution Vulnerability CVE ID : CVE-2023- 24905	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24905	O-MIC-WIND- 170523/2229		
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24946	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24946	O-MIC-WIND- 170523/2230		
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24949	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24949	O-MIC-WIND- 170523/2231		
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability CVE ID : CVE-2023- 24901	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24901	0-MIC-WIND- 170523/2232		
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2233		
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 930 of 1106						

Page **930** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24939	ability/CVE- 2023-24939	
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability CVE ID : CVE-2023- 24940	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24940	O-MIC-WIND- 170523/2234
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability CVE ID : CVE-2023- 24942	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24942	O-MIC-WIND- 170523/2235
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability CVE ID : CVE-2023- 29325	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29325	O-MIC-WIND- 170523/2236
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	O-MIC-WIND- 170523/2237
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24948	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24948	O-MIC-WIND- 170523/2238
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability CVE ID : CVE-2023- 24932	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24932	O-MIC-WIND- 170523/2239
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information	https://msrc .microsoft.co	O-MIC-WIND- 170523/2240

0-1

1-2

2-33-44-5Page 931 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			Disclosure Vulnerability CVE ID : CVE-2023- 24944	m/update- guide/vulner ability/CVE- 2023-24944			
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29324	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29324	0-MIC-WIND- 170523/2241		
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability CVE ID : CVE-2023- 24900	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24900	O-MIC-WIND- 170523/2242		
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability CVE ID : CVE-2023- 24945	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24945	O-MIC-WIND- 170523/2243		
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability CVE ID : CVE-2023- 28251	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28251	O-MIC-WIND- 170523/2244		
Product: windows_10_21h2							
Affected Ver	sion(s): * Up to (	excluding)	10.0.19044.2965				
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24943	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24943	O-MIC-WIND- 170523/2245		

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	8.8	Windows Bluetooth Driver Remote Code Execution Vulnerability CVE ID : CVE-2023- 24947	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24947	O-MIC-WIND- 170523/2246
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24903	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24903	O-MIC-WIND- 170523/2247
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability <b>CVE ID : CVE-2023- 28283</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28283	0-MIC-WIND- 170523/2248
N/A	09-May-2023	7.8	Remote Desktop Client Remote Code Execution Vulnerability CVE ID : CVE-2023- 24905	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24905	O-MIC-WIND- 170523/2249
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24946	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24946	O-MIC-WIND- 170523/2250
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc .microsoft.co m/update-	0-MIC-WIND- 170523/2251

0-1

1-2

2-33-44-5Page 933 of 1106

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24949	guide/vulner ability/CVE- 2023-24949	
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability CVE ID : CVE-2023- 24901	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24901	O-MIC-WIND- 170523/2252
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability CVE ID : CVE-2023- 24939	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24939	O-MIC-WIND- 170523/2253
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability <b>CVE ID : CVE-2023-</b> <b>24940</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24940	O-MIC-WIND- 170523/2254
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability CVE ID : CVE-2023- 24942	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24942	O-MIC-WIND- 170523/2255
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability CVE ID : CVE-2023- 29325	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29325	O-MIC-WIND- 170523/2256
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	O-MIC-WIND- 170523/2257

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24948	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24948	O-MIC-WIND- 170523/2258
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability CVE ID : CVE-2023- 24932	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24932	O-MIC-WIND- 170523/2259
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information Disclosure Vulnerability CVE ID : CVE-2023- 24944	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24944	O-MIC-WIND- 170523/2260
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29324	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29324	O-MIC-WIND- 170523/2261
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability CVE ID : CVE-2023- 24900	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24900	O-MIC-WIND- 170523/2262
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability CVE ID : CVE-2023- 24945	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24945	0-MIC-WIND- 170523/2263
N/A	09-May-2023	5.5	Windows Driver Revocation List	https://msrc .microsoft.co	0-MIC-WIND- 170523/2264

0-1

1-2

**2-3** 3-4 4-5 Page **935** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
			Security Feature Bypass Vulnerability CVE ID : CVE-2023-	m/update- guide/vulner ability/CVE- 2023-28251					
Droduct, wi	ndows 10 22h2		28251						
	Product: windows_10_22h2 Affected Version(s): * Up to (excluding) 10.0.19045.2965								
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24943	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24943	O-MIC-WIND- 170523/2265				
N/A	09-May-2023	8.8	Windows Bluetooth Driver Remote Code Execution Vulnerability CVE ID : CVE-2023- 24947	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24947	O-MIC-WIND- 170523/2266				
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24903	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24903	O-MIC-WIND- 170523/2267				
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability <b>CVE ID : CVE-2023- 28283</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28283	0-MIC-WIND- 170523/2268				

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.8	Remote Desktop Client Remote Code Execution Vulnerability CVE ID : CVE-2023- 24905	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24905	O-MIC-WIND- 170523/2269
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24946	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24946	O-MIC-WIND- 170523/2270
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24949	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24949	O-MIC-WIND- 170523/2271
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability CVE ID : CVE-2023- 24901	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24901	O-MIC-WIND- 170523/2272
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability CVE ID : CVE-2023- 24939	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24939	O-MIC-WIND- 170523/2273
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability <b>CVE ID : CVE-2023-</b> <b>24940</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24940	O-MIC-WIND- 170523/2274
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial	https://msrc .microsoft.co m/update- guide/vulner	0-MIC-WIND- 170523/2275

0-1

1-2

**2-3** 3-4 4-5 Page **937** of **1106**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Service Vulnerability	ability/CVE- 2023-24942	
			CVE ID : CVE-2023- 24942		
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability CVE ID : CVE-2023- 29325	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29325	O-MIC-WIND- 170523/2276
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	O-MIC-WIND- 170523/2277
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24948	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24948	O-MIC-WIND- 170523/2278
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability CVE ID : CVE-2023- 24932	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24932	O-MIC-WIND- 170523/2279
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information Disclosure Vulnerability CVE ID : CVE-2023- 24944	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24944	O-MIC-WIND- 170523/2280
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29324	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29324	O-MIC-WIND- 170523/2281

0-1

1-2

**2-3** 3-4 4-5 Page **938** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability CVE ID : CVE-2023- 24900	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24900	O-MIC-WIND- 170523/2282
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability CVE ID : CVE-2023- 24945	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24945	O-MIC-WIND- 170523/2283
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability CVE ID : CVE-2023- 28251	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28251	O-MIC-WIND- 170523/2284
Product: wi	ndows_11_21h2				
Affected Ver	sion(s): * Up to (e	excluding)	10.0.19044.2965		
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability CVE ID : CVE-2023- 24901	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24901	0-MIC-WIND- 170523/2285
Affected Ver	sion(s): * Up to (	excluding)	10.0.22000.1702	I	l
Concurrent Execution using Shared Resource with Improper Synchroniz ation	09-May-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24899	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24899	0-MIC-WIND- 170523/2286

0-1

1-2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
Affected Ver	sion(s): * Up to (e	excluding)	10.0.22000.1936		
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24943	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24943	0-MIC-WIND- 170523/2287
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 28283	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28283	O-MIC-WIND- 170523/2288
N/A	09-May-2023	7.8	Win32k Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24902	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24902	O-MIC-WIND- 170523/2289
N/A	09-May-2023	7.8	Remote Desktop Client Remote Code Execution Vulnerability CVE ID : CVE-2023- 24905	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24905	O-MIC-WIND- 170523/2290
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24946	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24946	O-MIC-WIND- 170523/2291
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc .microsoft.co m/update-	0-MIC-WIND- 170523/2292

0-1

1-2

**2-3** 3-4 4-5 Page **940** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24949	guide/vulner ability/CVE- 2023-24949	
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability CVE ID : CVE-2023- 24939	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24939	0-MIC-WIND- 170523/2293
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability <b>CVE ID : CVE-2023-</b> <b>24940</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24940	0-MIC-WIND- 170523/2294
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability CVE ID : CVE-2023- 24942	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24942	0-MIC-WIND- 170523/2295
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability CVE ID : CVE-2023- 29325	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29325	O-MIC-WIND- 170523/2296
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	O-MIC-WIND- 170523/2297
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24948	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24948	O-MIC-WIND- 170523/2298

1-2

	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability CVE ID : CVE-2023-	https://msrc .microsoft.co m/update- guide/vulner ability/CVE-	O-MIC-WIND- 170523/2299		
			24932	2023-24932			
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information Disclosure Vulnerability	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2300		
			CVE ID : CVE-2023- 24944	ability/CVE- 2023-24944			
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability <b>CVE ID : CVE-2023-</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE-	O-MIC-WIND- 170523/2301		
			29324	2023-29324			
N/A	09-May-2023	9-May-2023 5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability	https://msrc .microsoft.co m/update- guide/vulner ability/CVE-	O-MIC-WIND- 170523/2302		
				CVE ID : CVE-2023- 24900	2023-24900		
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability CVE ID : CVE-2023-	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24945	O-MIC-WIND- 170523/2303		
			24945	2023-24743			
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2304		
			CVE ID : CVE-2023- 28251	ability/CVE- 2023-28251			
Product: windows_11_22h2							
Affected Version(s): * Up to (excluding) 10.0.22000.1702							
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4 4-5 5-6	6-7 7-8	<u> </u>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24943	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24943	0-MIC-WIND- 170523/2305
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24903	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24903	0-MIC-WIND- 170523/2306
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability <b>CVE ID : CVE-2023- 28283</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28283	O-MIC-WIND- 170523/2307
N/A	09-May-2023	7.8	Win32k Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24902	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24902	O-MIC-WIND- 170523/2308
N/A	09-May-2023	7.8	Remote Desktop Client Remote Code Execution Vulnerability CVE ID : CVE-2023- 24905	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24905	O-MIC-WIND- 170523/2309
N/A	09-May-2023	7.8	Windows Backup Service Elevation of	https://msrc .microsoft.co	0-MIC-WIND- 170523/2310

0-1

1-2

2-3 3-4 4-5 Page **943** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability CVE ID : CVE-2023- 24946	m/update- guide/vulner ability/CVE- 2023-24946	
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24949	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24949	O-MIC-WIND- 170523/2311
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability CVE ID : CVE-2023- 24901	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24901	O-MIC-WIND- 170523/2312
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability CVE ID : CVE-2023- 24939	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24939	O-MIC-WIND- 170523/2313
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability CVE ID : CVE-2023- 24940	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24940	O-MIC-WIND- 170523/2314
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability CVE ID : CVE-2023- 24942	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24942	O-MIC-WIND- 170523/2315
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2316

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29325	ability/CVE- 2023-29325	
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	O-MIC-WIND- 170523/2317
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	09-May-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24899	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24899	O-MIC-WIND- 170523/2318
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability CVE ID : CVE-2023- 24932	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24932	O-MIC-WIND- 170523/2319
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information Disclosure Vulnerability CVE ID : CVE-2023- 24944	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24944	O-MIC-WIND- 170523/2320
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29324	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29324	O-MIC-WIND- 170523/2321
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information	https://msrc .microsoft.co m/update- guide/vulner	0-MIC-WIND- 170523/2322

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability	ability/CVE- 2023-24900	
			CVE ID : CVE-2023- 24900		
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability CVE ID : CVE-2023- 24945	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24945	O-MIC-WIND- 170523/2323
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability CVE ID : CVE-2023- 28251	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28251	O-MIC-WIND- 170523/2324
Product: wi	ndows_server_2	008		1	
Affected Ver	sion(s): -				
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24943	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24943	0-MIC-WIND- 170523/2325
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24903	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24903	O-MIC-WIND- 170523/2326
N/A	09-May-2023	8.1	Windows Lightweight Directory Access	https://msrc .microsoft.co m/update-	O-MIC-WIND- 170523/2327

0-1

1-2

**2-3** 3-4 4-5 Page **946** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol (LDAP) Remote Code Execution Vulnerability	guide/vulner ability/CVE- 2023-28283	
			CVE ID : CVE-2023- 28283		
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2328
			CVE ID : CVE-2023- 24940	ability/CVE- 2023-24940	
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability	https://msrc .microsoft.co m/update- guide/vulner	0-MIC-WIND- 170523/2329
			CVE ID : CVE-2023- 24942	ability/CVE- 2023-24942	
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability CVE ID : CVE-2023- 29325	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29325	O-MIC-WIND- 170523/2330
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	0-MIC-WIND- 170523/2331
N/A	09-May-2023	7.1	Windows Installer Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24904	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24904	O-MIC-WIND- 170523/2332
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2333

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24932	ability/CVE- 2023-24932	
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29324	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29324	O-MIC-WIND- 170523/2334
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability CVE ID : CVE-2023- 24900	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24900	0-MIC-WIND- 170523/2335
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability CVE ID : CVE-2023- 24945	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24945	O-MIC-WIND- 170523/2336
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability CVE ID : CVE-2023- 28251	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28251	O-MIC-WIND- 170523/2337
Affected Ver	sion(s): r2				•
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24943	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24943	O-MIC-WIND- 170523/2338
Concurrent Execution using Shared	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2339

0-1

1-2

**2-3** 3-4 4-5 Page **948** of **1106**  7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchroniz ation ('Race Condition')			Execution Vulnerability CVE ID : CVE-2023- 24903	ability/CVE- 2023-24903	
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 28283	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28283	O-MIC-WIND- 170523/2340
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24946	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24946	O-MIC-WIND- 170523/2341
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability <b>CVE ID : CVE-2023-</b> <b>24940</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24940	O-MIC-WIND- 170523/2342
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability CVE ID : CVE-2023- 24942	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24942	O-MIC-WIND- 170523/2343
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability CVE ID : CVE-2023- 29325	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29325	O-MIC-WIND- 170523/2344

0-1

1-2

5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	0-MIC-WIND- 170523/2345
N/A	09-May-2023	7.1	Windows Installer Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24904	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24904	0-MIC-WIND- 170523/2346
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability CVE ID : CVE-2023- 24932	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24932	0-MIC-WIND- 170523/2347
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29324	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29324	0-MIC-WIND- 170523/2348
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability CVE ID : CVE-2023- 24900	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24900	0-MIC-WIND- 170523/2349
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability CVE ID : CVE-2023- 24945	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24945	0-MIC-WIND- 170523/2350
N/A	09-May-2023	5.5	Windows Driver Revocation List	https://msrc .microsoft.co m/update-	O-MIC-WIND- 170523/2351

0-1

1-2

**2-3** 3-4 4-5 Page **950** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Feature Bypass Vulnerability CVE ID : CVE-2023- 28251	guide/vulner ability/CVE- 2023-28251	
Product: wi	ndows_server_2	2012			
Affected Ver	sion(s): -				
N/A	09-May-2023	9.8	Windows Network File System Remote Code Execution Vulnerability <b>CVE ID : CVE-2023-</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE-	O-MIC-WIND- 170523/2352
			24941	2023-24941	
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24943	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24943	O-MIC-WIND- 170523/2353
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24903	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24903	0-MIC-WIND- 170523/2354
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 28283	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28283	0-MIC-WIND- 170523/2355

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability CVE ID : CVE-2023- 24901	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24901	0-MIC-WIND- 170523/2356
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability CVE ID : CVE-2023- 24939	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24939	O-MIC-WIND- 170523/2357
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability <b>CVE ID : CVE-2023-</b> <b>24940</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24940	O-MIC-WIND- 170523/2358
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability CVE ID : CVE-2023- 24942	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24942	O-MIC-WIND- 170523/2359
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability CVE ID : CVE-2023- 29325	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29325	O-MIC-WIND- 170523/2360
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	O-MIC-WIND- 170523/2361
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2362

0-1

1-2

2-33-44-5Page 952 of 1106

6-7 7-8

5-6

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability CVE ID : CVE-2023- 24948	ability/CVE- 2023-24948	
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability CVE ID : CVE-2023- 24932	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24932	0-MIC-WIND- 170523/2363
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29324	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29324	O-MIC-WIND- 170523/2364
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability CVE ID : CVE-2023- 24900	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24900	0-MIC-WIND- 170523/2365
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability CVE ID : CVE-2023- 24945	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24945	O-MIC-WIND- 170523/2366
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability CVE ID : CVE-2023- 28251	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28251	O-MIC-WIND- 170523/2367
Affected Ver	rsion(s): r2		· · · · · · · · · · · · · · · · · · ·		
N/A	09-May-2023	9.8	Windows Network File System Remote	https://msrc .microsoft.co m/update-	0-MIC-WIND- 170523/2368

2-3 Page **953** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability CVE ID : CVE-2023- 24941	guide/vulner ability/CVE- 2023-24941	
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24943	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24943	O-MIC-WIND- 170523/2369
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24903	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24903	0-MIC-WIND- 170523/2370
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 28283	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28283	0-MIC-WIND- 170523/2371
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability CVE ID : CVE-2023- 24901	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24901	O-MIC-WIND- 170523/2372
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability	https://msrc .microsoft.co m/update-	O-MIC-WIND- 170523/2373

0-1

1-2

**2-3** 3-4 4-5 Page **954** of **1106**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24939	guide/vulner ability/CVE- 2023-24939	
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability CVE ID : CVE-2023- 24940	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24940	O-MIC-WIND- 170523/2374
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability CVE ID : CVE-2023- 24942	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24942	O-MIC-WIND- 170523/2375
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability CVE ID : CVE-2023- 29325	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29325	O-MIC-WIND- 170523/2376
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	O-MIC-WIND- 170523/2377
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24948	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24948	O-MIC-WIND- 170523/2378
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability CVE ID : CVE-2023- 24932	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24932	O-MIC-WIND- 170523/2379

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29324	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29324	O-MIC-WIND- 170523/2380
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability CVE ID : CVE-2023- 24900	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24900	0-MIC-WIND- 170523/2381
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability CVE ID : CVE-2023- 24945	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24945	O-MIC-WIND- 170523/2382
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability <b>CVE ID : CVE-2023-</b> <b>28251</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28251	O-MIC-WIND- 170523/2383
Product: wi	ndows_server_2	016			
Affected Ver	sion(s): -				
N/A	09-May-2023	9.8	Windows Network File System Remote Code Execution Vulnerability CVE ID : CVE-2023- 24941	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24941	0-MIC-WIND- 170523/2384
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24943	O-MIC-WIND- 170523/2385
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b>	6-7 7-8	8 8-9 9-10

Page **956** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24943		
N/A	09-May-2023	8.8	Windows Bluetooth Driver Remote Code Execution Vulnerability CVE ID : CVE-2023- 24947	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24947	O-MIC-WIND- 170523/2386
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24903	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24903	O-MIC-WIND- 170523/2387
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 28283	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28283	O-MIC-WIND- 170523/2388
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24946	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24946	O-MIC-WIND- 170523/2389
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability CVE ID : CVE-2023- 24901	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24901	O-MIC-WIND- 170523/2390

0-1

1-2

**2-3** 3-4 4-5 Page **957** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability CVE ID : CVE-2023- 24939	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24939	O-MIC-WIND- 170523/2391
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability <b>CVE ID : CVE-2023-</b> <b>24940</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24940	O-MIC-WIND- 170523/2392
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability CVE ID : CVE-2023- 24942	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24942	0-MIC-WIND- 170523/2393
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability CVE ID : CVE-2023- 29325	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29325	O-MIC-WIND- 170523/2394
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	O-MIC-WIND- 170523/2395
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24948	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24948	O-MIC-WIND- 170523/2396
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability	https://msrc .microsoft.co m/update- guide/vulner	0-MIC-WIND- 170523/2397

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 24932	ability/CVE- 2023-24932	
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29324	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29324	O-MIC-WIND- 170523/2398
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability CVE ID : CVE-2023- 24900	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24900	O-MIC-WIND- 170523/2399
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability CVE ID : CVE-2023- 24945	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24945	O-MIC-WIND- 170523/2400
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability CVE ID : CVE-2023- 28251	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28251	O-MIC-WIND- 170523/2401
Product: wi	ndows_server_2	019			
Affected Ver	sion(s): -				
N/A	09-May-2023	9.8	Windows Network File System Remote Code Execution Vulnerability CVE ID : CVE-2023- 24941	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24941	O-MIC-WIND- 170523/2402
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2403
CVSS Scoring S	Scale 0-1	L-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
			Execution Vulnerability	ability/CVE- 2023-24943	
			CVE ID : CVE-2023- 24943		
N/A	09-May-2023	8.8	Windows Bluetooth Driver Remote Code Execution Vulnerability	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2404
			CVE ID : CVE-2023- 24947	ability/CVE- 2023-24947	
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24903	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24903	O-MIC-WIND- 170523/2405
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24946	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24946	O-MIC-WIND- 170523/2406
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24949	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24949	O-MIC-WIND- 170523/2407
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability CVE ID : CVE-2023- 24901	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24901	O-MIC-WIND- 170523/2408

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability CVE ID : CVE-2023- 24939	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24939	O-MIC-WIND- 170523/2409
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability <b>CVE ID : CVE-2023-</b> <b>24940</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24940	O-MIC-WIND- 170523/2410
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability CVE ID : CVE-2023- 24942	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24942	O-MIC-WIND- 170523/2411
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24948	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24948	O-MIC-WIND- 170523/2412
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability CVE ID : CVE-2023- 24932	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24932	O-MIC-WIND- 170523/2413
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information Disclosure Vulnerability CVE ID : CVE-2023- 24944	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24944	O-MIC-WIND- 170523/2414
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2415

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability	ability/CVE- 2023-24900	
			CVE ID : CVE-2023- 24900		
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability CVE ID : CVE-2023- 24945	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24945	O-MIC-WIND- 170523/2416
Product: wi	ndows_server_2	2022			
Affected Ver	sion(s): -				
N/A	09-May-2023	9.8	Windows Network File System Remote Code Execution Vulnerability CVE ID : CVE-2023- 24941	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24941	O-MIC-WIND- 170523/2417
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24943	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24943	O-MIC-WIND- 170523/2418
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 24903	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24903	O-MIC-WIND- 170523/2419
N/A	09-May-2023	8.1	Windows Lightweight Directory Access	https://msrc .microsoft.co m/update-	O-MIC-WIND- 170523/2420

0-1

1-2

**2-3** 3-4 4-5 Page **962** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol (LDAP) Remote Code Execution Vulnerability CVE ID : CVE-2023- 28283	guide/vulner ability/CVE- 2023-28283	
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24949	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24949	O-MIC-WIND- 170523/2421
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability CVE ID : CVE-2023- 24901	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24901	O-MIC-WIND- 170523/2422
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability CVE ID : CVE-2023- 24939	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24939	O-MIC-WIND- 170523/2423
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability <b>CVE ID : CVE-2023-</b> <b>24940</b>	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24940	O-MIC-WIND- 170523/2424
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability CVE ID : CVE-2023- 24942	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24942	O-MIC-WIND- 170523/2425
N/A	09-May-2023	7.5	Windows OLE Remote Code	https://msrc .microsoft.co m/update- guide/vulner	O-MIC-WIND- 170523/2426
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>963</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Page 963 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability CVE ID : CVE-2023- 29325	ability/CVE- 2023-29325	
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29335	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29335	O-MIC-WIND- 170523/2427
Concurrent Execution using Shared Resource with Improper Synchroniz ation ('Race Condition')	09-May-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability CVE ID : CVE-2023- 24899	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24899	0-MIC-WIND- 170523/2428
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability CVE ID : CVE-2023- 24932	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24932	O-MIC-WIND- 170523/2429
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information Disclosure Vulnerability CVE ID : CVE-2023- 24944	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24944	O-MIC-WIND- 170523/2430
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability CVE ID : CVE-2023- 29324	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-29324	O-MIC-WIND- 170523/2431
N/A	09-May-2023	5.9	Windows NTLM Security Support	https://msrc .microsoft.co	0-MIC-WIND- 170523/2432

0-1

1-2

**2-3** 3-4 4-5 Page **964** of **1106**  6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Provider Information Disclosure Vulnerability CVE ID : CVE-2023- 24900	m/update- guide/vulner ability/CVE- 2023-24900	
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability CVE ID : CVE-2023- 24945	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24945	0-MIC-WIND- 170523/2433
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability CVE ID : CVE-2023- 28251	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-28251	O-MIC-WIND- 170523/2434
Affected Ver	sion(s): * Up to (e	excluding)	10.0.20348.1724		
N/A	09-May-2023	7.5	Windows SMB Denial of Service Vulnerability CVE ID : CVE-2023- 24898	https://msrc .microsoft.co m/update- guide/vulner ability/CVE- 2023-24898	O-MIC-WIND- 170523/2435
Vendor: mil	esight				
Product: nc	r\/camera_firm	ware			
Affected Ver	sion(s): 71.8.0.6-	r5			-
N/A	08-May-2023	7.5	Milesight NCR/camera version 71.8.0.6-r5 discloses sensitive information through an unspecified request.	N/A	O-MIL-NCR\- 170523/2436
			CVE ID : CVE-2023- 24505		
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>
ŭ			Page <b>965</b> of <b>1106</b>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Insufficient ly Protected Credentials	08-May-2023	7.5	Milesight NCR/camera version 71.8.0.6-r5 exposes credentials through an unspecified request.	N/A	O-MIL-NCR\- 170523/2437		
			CVE ID : CVE-2023- 24506				
Vendor: mit	trastar						
Product: gp	t-2741gnac-n2_	firmware	;				
Affected Ver	sion(s): br_g5.9_2	l.11\\(wv	vk.0\\)b32				
N/A	05-May-2023	8.8	MitraStar GPT- 2741GNAC-N2 with firmware BR_g5.9_1.11(WVK.0) )b32 was discovered to contain a remote code execution (RCE) vulnerability in the ping function. <b>CVE ID : CVE-2023-</b>	N/A	O-MIT-GPT 170523/2438		
			30065				
Vendor: Qua	alcomm						
Product: 31	Product: 315_5g_iot_modem_firmware						
Affected Version(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	0-QUA-315 170523/2439		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			-	0.00	64400					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023- bulletin	
Product: 89	05_firmware				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-8905- 170523/2440
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-8905- 170523/2441
Product: 89	09_firmware				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-8909- 170523/2442
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-8909- 170523/2443
Product: 89	17_firmware				
Affected Vers	sion(s): -				

0-1

1-2

5-6

6-7 7-8

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-8917- 170523/2444
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-8917- 170523/2445
Product: 89	52_firmware				
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-8952- 170523/2446
Product: 89	53pro_firmware	e			
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-8953- 170523/2447
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	0-QUA-8953- 170523/2448

0-1

1-2

**2-3** 3-4 4-5 Page **968** of **1106**  6-7 7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin	
Product: 89	53_firmware				
Affected Ver	sion(s): -				_
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-8953- 170523/2449
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-8953- 170523/2450
Product: 89	56_firmware			I	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-8956- 170523/2451
Product: 89	76pro_firmwar	e			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	0-QUA-8976- 170523/2452

CVSS	Scoring	Scale	
------	---------	-------	--

1-2

2-3

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023- bulletin	
Product: 89	76_firmware				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-8976- 170523/2453
Product: 89	98_firmware				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-8998- 170523/2454
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-8998- 170523/2455
Product: 92	06_lte_modem_	firmware		I	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-9206- 170523/2456

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Product: apq5053-aa_firmware								
Affected Version(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-APQ5- 170523/2457			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-APQ5- 170523/2458			
Product: ap	q8017_firmwar	e		<u>I</u>				
Affected Vers	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-APQ8- 170523/2459			
Product: apq8052_firmware								
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-APQ8- 170523/2460			
Product: apq8053-aa_firmware								
Affected Version(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 971 of 1106								

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-APQ8- 170523/2461			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-APQ8- 170523/2462			
Product: apq8053-ac_firmware								
Affected Version(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-APQ8- 170523/2463			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-APQ8- 170523/2464			
Product: ap	q8053-lite_firm	ware						
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull	O-QUA-APQ8- 170523/2465			
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10           Page 972 of 1106								

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-APQ8- 170523/2466
	q8056_firmwar	e			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-APQ8- 170523/2467
Product: ap	q8064au_firmw	are			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-APQ8- 170523/2468
Product: ap	q8076_firmwar	e			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	0-QUA-APQ8- 170523/2469

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
				2023- bulletin		
Product: aq	t1000_firmware	e		·		
Affected Vers	sion(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-AQT1- 170523/2470	
Product: ar	8031_firmware					
Affected Ver	sion(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-AR80- 170523/2471	
Product: ar	8035_firmware			l		
Affected Ver	sion(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-AR80- 170523/2472	
Product: c-v	2x_9150_firmw	are		<u></u>		
Affected Version(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	0-QUA-C-V2- 170523/2473	
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b>	5 6-7 7-8	8 8-9 9-10	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023- bulletin	
Product: csi	ra6620_firmwai	·e		·	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-CSRA- 170523/2474
Product: csi	ra6640_firmwai	·e		<u></u>	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-CSRA- 170523/2475
Product: csi	rb31024_firmwa	are	L	1	I
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-CSRB- 170523/2476
Product: flig	ght_rb5_5g_plat	form_firm	iware	<u></u>	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	0-QUA-FLIG- 170523/2477
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b>	5 6-7 7-8	3 8-9 9 <b>-10</b>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-FLIG- 170523/2478
Product: ho	me_hub_100_pla	atform_fi	rmware		
Affected Vers	sion(s): -				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-HOME- 170523/2479
Product: mo	lm9250_firmwa	re			
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-MDM9- 170523/2480
Missing Release of Memory		7.8	Memory Corruption in Graphics while accessing a buffer allocated through the	https://ww w.qualcomm .com/compa ny/product- security/bull	0-QUA-MDM9- 170523/2481
after Effective Lifetime	02-May-2023		graphics pool. CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin	
Effective Lifetime	02-May-2023 1m9628_firmwa	ıre	CVE ID : CVE-2023-	2023-	

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-MDM9- 170523/2482
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-MDM9- 170523/2483
Product: mo	dm9650_firmwa	re			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-MDM9- 170523/2484
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-MDM9- 170523/2485
Product: ms	sm8108_firmwa	re			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull	0-QUA-MSM8- 170523/2486
CVSS Scoring S	Scale 0-1 C	1-2 2-3	3-4 4-5 5-6 Page <b>977</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-MSM8- 170523/2487
Product: ms	sm8209_firmwa	re			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-MSM8- 170523/2488
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-MSM8- 170523/2489
Product: ms	sm8608_firmwa	re			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-MSM8- 170523/2490

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-MSM8- 170523/2491
Product: ms	sm8909w_firmw	vare			
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-MSM8- 170523/2492
Product: ms	sm8996au_firm	ware			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-MSM8- 170523/2493
Product: qa	m8295p_firmwa	are			
Affected Ver	sion(s): -				
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. CVE ID : CVE-2023- 21642	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-QAM8- 170523/2494

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QAM8- 170523/2495			
-	a-4020-0-217m	sp_firmw	are					
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA 170523/2496			
Product: qc	a-4020-1-217m	sp_firmw	are					
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA 170523/2497			
Product: qc	a-4024-0-68cm	qfn_firmw	vare					
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA 170523/2498			
Product: qc	Product: qca-4024-1-68cmqfn_firmware							
Affected Ver	Affected Version(s): -							
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>980</b> of <b>1106</b>	6-7 7-8	8 8-9 <mark>9-10</mark>			

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA 170523/2499
Product: qc	a6174a_firmwa	re			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2500
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2501
Product: qc	a6174_firmware	e		I	
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2502
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	0-QUA-QCA6- 170523/2503

0-1

1-2

2-33-44-5Page 981 of 1106

6-7 7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin	
Product: qc	a6310_firmwar	9			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2504
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2505
Product: qc	a6320_firmwar	9			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2506
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2507
Product: qc	a6335_firmwar	e			

0-1

1-2

**2-3** 3-4 4-5 Page **982** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Affected Ver	Affected Version(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2508				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2509				
Product: qc	a6390_firmwar	e							
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2510				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2511				
Product: qc	a6391_firmwar	e			1				
Affected Ver	sion(s): -								
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product-	0-QUA-QCA6- 170523/2512				
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				
CV00 SCOTTING S		- 2 - 3	J J- J-						

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Conversion or Cast			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2513				
Product: qc	a6420_firmwar	9							
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2514				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2515				
Product: qc	Product: qca6421_firmware								
Affected Ver	Affected Version(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-QCA6- 170523/2516				

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2517
Product: qc	a6426_firmware	9			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2518
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2519
Product: qc	a6430_firmware	e			I
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2520
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	0-QUA-QCA6- 170523/2521

0-1

1-2

**2-3** 3-4 4-5 Page **985** of **1106**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin						
Product: qca6431_firmware										
Affected Ver	sion(s): -		1	1	1					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2522					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2523					
Product: qc	a6436_firmwar	9		I						
Affected Ver	sion(s): -									
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2524					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2525					
Product: qc	a6564au_firmw	are								

0-1

1-2

**2-3** 3-4 4-5 Page **986** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2526
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2527
Product: qc	a6564a_firmwa	re			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2528
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2529
Product: qc	a6564_firmwar	e			
Affected Ver	sion(s): -				
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product-	0-QUA-QCA6- 170523/2530
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5	-6 6-7 7-8	8 8-9 <mark>9-10</mark>
CARR 200		I-Z Z-3	5-4 4-5 5	0 0-7 7-6	0 0-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Conversion or Cast			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2531		
Product: qca	a6574au_firmwa	are					
Affected Vers	sion(s): -						
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. CVE ID : CVE-2023- 21642	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2532		
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2533		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2534		
Product: qca6574a_firmware							
Affected Vers	sion(s): -						

0-1

1-2

2-3

3-44-5Page 988 of 1106

6-7 7-8

5-6

Incorrect Type Conversion or Cast02-May-20237.8in Gr impor CVE 2166Missing Release of Memory after Effective Lifetime02-May-20237.8Mem in Gr acces alloc grap CVE 2166Product: qca5774_firmwareVAffected Version(s): -VVIncorrect Type Conversion or Cast02-May-20237.8Mem in Gr acces alloc grap CVE 2166Missing Release of Memory after Effective Lifetime02-May-20237.8Mem in Gr in GrMissing Release of Memory after Effective Lifetime02-May-20237.8Mem in Gr in Gr in Gr in Gr in Gr in GrMissing Release of Memory after Effective Lifetime02-May-20237.8Mem in Gr in Gr in Gr in Gr in GrMissing Conversion O2-May-20237.8Mem in Gr in Gr	escription & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime02-May-20237.8in Gr acces alloc grapher CVE 2166Product: qc=574_firmwareVAffected Version(s): -Mem in Gr in Gr<	nory corruption araphics while oorting a file. E ID : CVE-2023- 565	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2535
Affected Version(s): -Incorrect Type Conversion or Cast02-May-20237.8Mem in Gr impo CVE 2166Missing Release of Memory after Effective Lifetime02-May-20237.8Mem in Gr acces alloc graph CVE 2166Product: qca584au_firmw=reVVVAffected Version(s): -02-May-20237.8Mem in Gr acces alloc graph CVE 2166Incorrect Type Conversion or Cast02-May-20237.8Mem in Gr in Gr in Gr in Gr in Gr in Gr in Gr in Gr in Gr 	nory Corruption Fraphics while essing a buffer cated through the phics pool. E ID : CVE-2023- 566	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2536
Incorrect Type Conversion or Cast02-May-20237.8Mem in Gr impo CVE 2166Missing Release of Memory after Effective Lifetime02-May-20237.8Mem in Gr acces alloc graph CVE 2166Product: qca6584au_firmw=rect Type Conversion or Cast02-May-20237.8Mem in Gr acces alloc graph CVE 2166			
Incorrect Type Conversion or Cast02-May-20237.8in Gr impo CVE 2166Missing Release of Memory after Effective Lifetime02-May-20237.8Mem in Gr acces alloc graphProduct: qca6584au_firmwreCVE 2166Product: qca6584au_firmwreCVE alloc graphAffected Version(s): -Mem in Gr in Gr			
Missing Release of Memory after Effective Lifetime Product: qca6584au_firmware Affected Version(s): - Incorrect Type Conversion or Cast	nory corruption graphics while porting a file. E <b>ID : CVE-2023-</b> 565	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2537
Affected Version(s): - Incorrect Type Conversion or Cast	nory Corruption Fraphics while essing a buffer cated through the phics pool. E ID : CVE-2023- 566	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2538
Incorrect Type Conversion or Cast 02-May-2023 7.8 Mem in Gr impo <b>CVE</b>			
Incorrect Type Conversion or Cast In Gr in Gr in Gr impo CVE			
	nory corruption craphics while orting a file. E ID : CVE-2023- 565	https://ww w.qualcomm .com/compa ny/product- security/bull	0-QUA-QCA6- 170523/2539
	<mark>3-4 4-5 5-6</mark> e <b>989</b> of <b>1106</b>	6-7 7-8	8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may- 2023- bulletin	
Product: qc	a6595au_firmw	are			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2540
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2541
Product: qc	a6595_firmware	e		<u> </u>	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2542
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2543
Product: qc	a6696_firmware	e			

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Affected Version(s): -								
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2544			
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2545			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2546			
Product: qc	a6698aq_firmw	are			<u> </u>			
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA6- 170523/2547			
Product: qca8081_firmware								
Affected Version(s): -								
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa	0-QUA-QCA8- 170523/2548			

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Р	age <b>991</b> o	f <b>1106</b>					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			CVE ID : CVE-2023- 21665	ny/product- security/bull etins/may- 2023- bulletin	
Product: qc	a8337_firmware	9			
Affected Ver	sion(s): -				-
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA8- 170523/2549
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA8- 170523/2550
Product: qc	a9367_firmware	9			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA9- 170523/2551
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA9- 170523/2552

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID						
Product: qc	a9377_firmwar	e		I							
Affected Ver	Affected Version(s): -										
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA9- 170523/2553						
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA9- 170523/2554						
Product: qc	a9379_firmware	9									
Affected Ver	sion(s): -										
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA9- 170523/2555						
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCA9- 170523/2556						
	Product: qcm2290_firmware										
Affected Ver	sion(s): -										

0-1

1-2

**2-3** 3-4 4-5 Page **993** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCM2- 170523/2557			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-QCM2- 170523/2558			
Product: qc	m4290_firmwai	·e						
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-QCM4- 170523/2559			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-QCM4- 170523/2560			
Product: qc	m6125_firmwai	·e						
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull	O-QUA-QCM6- 170523/2561			
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 994 of 1106							

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
				etins/may- 2023- bulletin				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCM6- 170523/2562			
	m6490_firmwar	е						
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCM6- 170523/2563			
Product: qc	n6024_firmwar	e						
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCN6- 170523/2564			
Product: qc	n9011_firmwar	e						
Affected Ver	Affected Version(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	0-QUA-QCN9- 170523/2565			

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCN9- 170523/2566
Product: qc	n9012_firmwar	9			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCN9- 170523/2567
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCN9- 170523/2568
Product: qc	n9024_firmwar	9			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCN9- 170523/2569
Product: qc	n9074_firmwar	e			
Affected Ver	sion(s): -				

0-1

1-2

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCN9- 170523/2570
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCN9- 170523/2571
Product: qc	s2290_firmware	9			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-QCS2- 170523/2572
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCS2- 170523/2573
Product: qc	s400_firmware				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull	0-QUA-QCS4- 170523/2574
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>997</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may- 2023- bulletin	
Product: qc	s410_firmware				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCS4- 170523/2575
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCS4- 170523/2576
Product: qc	s4290_firmware	9			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCS4- 170523/2577
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCS4- 170523/2578
Product: qc	s605_firmware				

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
Affected Ver	sion(s): -									
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCS6- 170523/2579					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCS6- 170523/2580					
Product: qc	Product: qcs610_firmware									
Affected Ver	sion(s): -									
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCS6- 170523/2581					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCS6- 170523/2582					
Product: qc	s6125_firmware	9								
Affected Ver	sion(s): -									
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product-	0-QUA-QCS6- 170523/2583					
			3-4 4-5 5	-6 6-7 7-8						
CVSS Scoring S	Scale 0-1	1-2 2-3	5-4 4-5 5	-0 0-7 7-8	8 8-9 9-10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCS6- 170523/2584
Product: qc	s6490_firmware	e			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCS6- 170523/2585
Product: qc	s8155_firmware	e			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCS8- 170523/2586
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCS8- 170523/2587

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Product: qcs8250_firmware									
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCS8- 170523/2588				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QCS8- 170523/2589				
Product: qn	Product: qm215_firmware								
Affected Ver	sion(s): -								
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QM21- 170523/2590				
Product: qr	b5165m_firmwa	are		I					
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-QRB5- 170523/2591				
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://ww w.qualcomm	0-QUA-QRB5- 170523/2592				

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

		accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	.com/compa ny/product- security/bull etins/may- 2023- bulletin	
	re			
sion(s): -			ſ	1
02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-QRB5- 170523/2593
02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QRB5- 170523/2594
b5165_firmwar	e	<u> </u>		<u> </u>
sion(s): -				
02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-QRB5- 170523/2595
02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	O-QUA-QRB5- 170523/2596
	sion(s): -         02-May-2023         02-May-2023         b5165_firmwar         sion(s): -         02-May-2023	02-May-2023 7.8 02-May-2023 7.8 b5165_firmware sion(s): - 02-May-2023 7.8	graphics pool. CVE ID : CVE-2023- 21666b5165n_firmwaresion(s): -02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 2166502-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666b5165_firmwaresion(s): -02-May-20237.8Memory corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666b5165_firmwaresion(s): -02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 2166502-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.02-May-20237.8Memory Corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	graphics pool. CVE ID : CVE-2023- 21666security/bull etins/may- 2023- bulletinb5165n_firmwaresion(s): -02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin02-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinb5165_firmwaresion(s): -02-May-20237.8Memory corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin02-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.02-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.02-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.

Page 1002 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
				2023- bulletin					
Product: qs	Product: qsm8250_firmware								
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-QSM8- 170523/2597				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-QSM8- 170523/2598				
Product: sa	4150p_firmware	9							
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA41- 170523/2599				
Product: sa	4155p_firmware	9							
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SA41- 170523/2600				

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sa	6145p_firmware	9			
Affected Vers	sion(s): -				
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. CVE ID : CVE-2023- 21642	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA61- 170523/2601
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA61- 170523/2602
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA61- 170523/2603
Product: sa	6150p_firmware	9			
Affected Vers	sion(s): -				
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. CVE ID : CVE-2023- 21642	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA61- 170523/2604
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product- security/bull	0-QUA-SA61- 170523/2605
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4 4-5 5-6	6-7 7-8	8 8-9 <mark>9-10</mark>

after Effective Lifetime02-May-20237.8anocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b> security/bull etins/may- 2023- bulletin170523/2606Product: sa6155p_firmwareAffected Version(s): -Memory corruption in HAB Memory management due to broad system privileges via physical address.https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime $0^{2}$ -May-2023 $7.8$					2023-	
Affected Version(s): -         Affected Version(s): -         N/A       02-May-2023         7.8       Memory corruption in HAB Memory management due to broad system privileges via physical address.       https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-         0-QUA-SA61- 170523/2602	Release of Memory after Effective	02-May-2023	7.8	in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b>	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-	0-QUA-SA61- 170523/2606
N/A 02-May-2023 7.8 Memory corruption in HAB Memory management due to broad system privileges via physical address. CVE ID : CVE-2023- locution https://ww w.qualcomm ny/product- security/bull tro523/2602 locution https://ww w.qualcomm ny/product- 2023-		<del>_</del>	e			
N/A 02-May-2023 7.8 in HAB Memory w.qualcomm broad system ny/product- privileges via security/bull 170523/2602 physical address. etins/may- CVE ID : CVE-2023- 2023-	Affected Vers	sion(s): -				1
<b>21642</b> bulletin	N/A	02-May-2023	7.8	in HAB Memory management due to broad system privileges via physical address.	w.qualcomm .com/compa ny/product- security/bull etins/may-	0-QUA-SA61- 170523/2607
	Type Conversion	02-May-2023	7.8	in Graphics while importing a file. <b>CVE ID : CVE-2023-</b>	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-	0-QUA-SA61- 170523/2608
	Release of Memory after Effective	02-May-2023	7.8	in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b>	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-	0-QUA-SA61- 170523/2609
Product: sa6155_firmware	Product: sat	6155_firmware				
Affected Version(s): -	Affected Vers	sion(s): -				

0-1

1-2

**2-3 3-4 4-5** Page **1005** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA61- 170523/2610				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA61- 170523/2611				
	Product: sa8145p_firmware								
Affected Ver	sion(s): -			1					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA81- 170523/2612				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA81- 170523/2613				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	0-QUA-SA81- 170523/2614				

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
				2023- bulletin					
Product: sa	Product: sa8150p_firmware								
Affected Ver	sion(s): -								
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA81- 170523/2615				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA81- 170523/2616				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA81- 170523/2617				
Product: sa	8155p_firmware	e							
Affected Ver	sion(s): -								
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA81- 170523/2618				

0-1

1-2

5-6

6-7 7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA81- 170523/2619
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA81- 170523/2620
Product: sa8155_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA81- 170523/2621
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA81- 170523/2622
Product: sa8195p_firmware					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system	https://ww w.qualcomm .com/compa ny/product- security/bull	0-QUA-SA81- 170523/2623

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
			privileges via physical address. CVE ID : CVE-2023- 21642	etins/may- 2023- bulletin			
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA81- 170523/2624		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SA81- 170523/2625		
Product: sa8295p_firmware							
Affected Ver	sion(s): -			1			
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA82- 170523/2626		
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA82- 170523/2627		
	8540p_firmware	e			•		
Affected Ver	sion(s): -						

0-1

1-2

**2-3 3-4 4-5** Page **1009** of **1106**  5-6

7-8

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA85- 170523/2628	
Product: sa	9000p_firmware	e				
Affected Version(s): -						
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. <b>CVE ID : CVE-2023-</b> <b>21642</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SA90- 170523/2629	
Product: sd	626_firmware					
Affected Vers	sion(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD62- 170523/2630	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD62- 170523/2631	
Product: sd	660_firmware		L		L	
Affected Vers	sion(s): -					

0-1

1-2

2-33-44-5Page 1010 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD66- 170523/2632	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD66- 170523/2633	
Product: sd	670_firmware					
Affected Version(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SD67- 170523/2634	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD67- 170523/2635	
Product: sd	675_firmware					
Affected Ver	sion(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull	O-QUA-SD67- 170523/2636	
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>1011</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
				etins/may- 2023- bulletin			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD67- 170523/2637		
	730_firmware						
Affected Ver	Affected Version(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD73- 170523/2638		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD73- 170523/2639		
Product: sd835_firmware							
Affected Ver	Affected Version(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD83- 170523/2640		

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD83- 170523/2641
Product: sd	855_firmware				
Affected Ver	sion(s): -				_
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD85- 170523/2642
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD85- 170523/2643
Product: sd	865_5g_firmwar	·e			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD86- 170523/2644
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	0-QUA-SD86- 170523/2645

0-1

1-2

**2-3** 3-4 4-5 Page **1013** of **1106**  8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin			
Product: sd	888_firmware						
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD88- 170523/2646		
Product: sd	a\/sdm845_firn	nware		I			
Affected Ver	Affected Version(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SDA\- 170523/2647		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SDA\- 170523/2648		
Product: sdm429w_firmware							
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	0-QUA-SDM4- 170523/2649		

CVSS	Scoring	Scale
------	---------	-------

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SDM4- 170523/2650
Product: sd	m429_firmware				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SDM4- 170523/2651
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SDM4- 170523/2652
Product: sd	m439_firmware	2			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SDM4- 170523/2653
Missing Release of Memory	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer	https://ww w.qualcomm .com/compa	0-QUA-SDM4- 170523/2654

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

Page 1015 of 1106

10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
after Effective Lifetime			allocated through the graphics pool. CVE ID : CVE-2023- 21666	ny/product- security/bull etins/may- 2023- bulletin	
Product: sd	m450_firmware				
Affected Ver	sion(s): -				_
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SDM4- 170523/2655
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SDM4- 170523/2656
Product: sd	<mark>m660_firmware</mark>				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SDM6- 170523/2657
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SDM6- 170523/2658

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Product: sd	m670_firmware					
Affected Ver	sion(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SDM6- 170523/2659	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SDM6- 170523/2660	
Product: sdm710_firmware						
Affected Ver	sion(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SDM7- 170523/2661	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SDM7- 170523/2662	
	m845_firmware			1		
Affected Ver	sion(s): -					

0-1

1-2

**2-3** 3-4 4-5 Page **1017** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SDM8- 170523/2663	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SDM8- 170523/2664	
Product: sd	x20m_firmware					
Affected Version(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SDX2- 170523/2665	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SDX2- 170523/2666	
Product: sd	x55_firmware					
Affected Ver	sion(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull	O-QUA-SDX5- 170523/2667	
CVSS Scoring S	Scale 0-1 C	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>1018</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SDX5- 170523/2668
Product: sd	_675_firmware				
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD_6- 170523/2669
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SD_6- 170523/2670
Product: sm	4125_firmware			L	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM41- 170523/2671

0-1

1-2

5-6

6-7

Missing Release of Memory after Effective Lifetime02-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinProduct: sm4250-aa_firmwareMemory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinIncorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinMissing Release of Memory after Lifetime02-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinMissing Release of Memory after Lifetime02-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinMissing Release of Memory after Lifetime02-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa .com/comp	0-QUA-SM42-						
Affected Version(s): -Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinMissing Release of Memory after Effective Lifetime02-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinProduct: sm4350-ac_firmware7.8Memory Corruption in Graphics while allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	v						
Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b> https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinMissing Release of Memory after Effective Lifetime02-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin <b>Product: sm4350-ac_firmwareVector</b> Memory Corruption in Graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b> https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	v						
Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file.w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinMissing Release of Memory after Effective Lifetime02-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinMissing Release of Memory after Effective Lifetime02-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinProduct: sm4350-ac_firmwareUUU	v						
Missing Release of Memory after Lifetime02-May-20237.8Memory corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinProduct: sm4350-ac_firmware							
	0-QUA-SM42- 170523/2674						
Affected Version(s): -							
Incorrect Type Conversion or Cast02-May-20237.8Memory corruption 	0-QUA-SM43- 170523/2675						
Product: sm4350_firmware							
Affected Version(s): -							

0-1

1-2

2-33-44-5Page 1020 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM43- 170523/2676
Product: sm	4375_firmware	!			
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM43- 170523/2677
Product: sm	16115_firmware	<u>!</u>			
Affected Vers	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM61- 170523/2678
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM61- 170523/2679
Product: sm Affected Vers	6125_firmware sion(s): -				

0-1

1-2

2-33-44-5Page 1021 of 1106

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM61- 170523/2680
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM61- 170523/2681
Product: sm	16150-ac_firmw	are			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM61- 170523/2682
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM61- 170523/2683
Product: sm	16150_firmware	!			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull	0-QUA-SM61- 170523/2684
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>1022</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM61- 170523/2685
Product: sm	16225-ad_firmw	are			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM62- 170523/2686
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM62- 170523/2687
Product: sm	6225_firmware			L	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SM62- 170523/2688

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM62- 170523/2689
	16250p_firmwar	'e			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM62- 170523/2690
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM62- 170523/2691
Product: sm	6250_firmware	2			I
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM62- 170523/2692
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	emory Corruption Graphics while cessing a buffer ocated through the ocated through the	

0-1

1-2

**2-3 3-4 4-5** Page **1024** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID					
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin						
Product: sm	Product: sm6350_firmware									
Affected Ver	Affected Version(s): -									
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM63- 170523/2694					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM63- 170523/2695					
Product: sm	16375_firmware			I						
Affected Ver	sion(s): -									
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM63- 170523/2696					
Product: sm	Product: sm7125_firmware									
Affected Ver	sion(s): -									
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	0-QUA-SM71- 170523/2697					

CVSS	Scoring	Scale
------	---------	-------

0-1

1-2

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM71- 170523/2698
Product: sm	7150-aa_firmw	are			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM71- 170523/2699
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM71- 170523/2700
Product: sm	7150-ab_firmw	are			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM71- 170523/2701
Missing Release of Memory	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer	https://ww w.qualcomm .com/compa	0-QUA-SM71- 170523/2702

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
after Effective Lifetime			allocated through the graphics pool. CVE ID : CVE-2023- 21666	ny/product- security/bull etins/may- 2023- bulletin	
Product: sm	7150-ac_firmwa	are			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM71- 170523/2703
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM71- 170523/2704
Product: sm	7225_firmware	<u>.</u>			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM72- 170523/2705
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM72- 170523/2706

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Product: sm	7250-aa_firmw	are	L	I	L			
Affected Version(s): -								
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM72- 170523/2707			
Product: sm	7250-ab_firmw	are						
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM72- 170523/2708			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM72- 170523/2709			
Product: sm	7250-ac_firmwa	are	L	I				
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM72- 170523/2710			
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://ww w.qualcomm	0-QUA-SM72- 170523/2711			

 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
Memory after Effective Lifetime			accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	.com/compa ny/product- security/bull etins/may- 2023- bulletin	
Product: sm	17250p_firmwai	·e			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SM72- 170523/2712
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM72- 170523/2713
Product: sm	17315_firmware	•			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SM73- 170523/2714
Product: sm	n7325-ae_firmw	are			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product-	0-QUA-SM73- 170523/2715

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Deep 1020 of 1100										

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin	
Product: sm	17325-af_firmwa	are		1	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SM73- 170523/2716
Product: sm	17325p_firmwa1	е			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM73- 170523/2717
Product: sm	7325_firmware	2	L	1	I
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM73- 170523/2718
Product: sm	7350-ab_firmw	are		<u> </u>	
Affected Ver	sion(s): -				
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product-	O-QUA-SM73- 170523/2719
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>1030</b> of <b>1106</b>	5 6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin	
Product: sm	18150-ac_firmwa	are			
Affected Ver	sion(s): -				_
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM81- 170523/2720
Product: sm	8150_firmware	;			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM81- 170523/2721
Product: sm	8250-ab_firmw	are			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM82- 170523/2722
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	0-QUA-SM82- 170523/2723

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
			CVE ID : CVE-2023- 21666	2023- bulletin				
Product: sm	Product: sm8250-ac_firmware							
Affected Ver	sion(s): -				-			
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM82- 170523/2724			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM82- 170523/2725			
Product: sm	18250_firmware			I				
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM82- 170523/2726			
Product: sm	18350-ac_firmwa	are						
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM83- 170523/2727			

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sm	18350_firmware	! !	L	I	L
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SM83- 170523/2728
Product: sn	apdragon_1200	wearabl	e_platform_firmware		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SNAP- 170523/2729
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SNAP- 170523/2730
Product: sn	apdragon_208_p	processor	_firmware		I
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SNAP- 170523/2731
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://ww w.qualcomm	0-QUA-SNAP- 170523/2732

 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		
Memory after Effective Lifetime			accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	.com/compa ny/product- security/bull etins/may- 2023- bulletin			
Product: sn	apdragon_630_1	nobile_pl	atform_firmware		•		
Affected Ver	sion(s): -				-		
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SNAP- 170523/2733		
Product: sn	Product: snapdragon_632_mobile_platform_firmware						
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SNAP- 170523/2734		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SNAP- 170523/2735		
Product: sn	apdragon_636_1	nobile_pl	atform_firmware				
Affected Ver	sion(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product-	0-QUA-SNAP- 170523/2736		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin	
Product: sn	apdragon_7c\+_	gen_3_co	mpute_firmware		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SNAP- 170523/2737
Product: sn	apdragon_820_a	utomotiv	ve_platform_firmware		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SNAP- 170523/2738
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SNAP- 170523/2739
Product: sn	apdragon_auto_	4g_mode	m_firmware		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	O-QUA-SNAP- 170523/2740

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SNAP- 170523/2741
Product: sn	apdragon_auto_	5g_mode	m-rf_firmware		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SNAP- 170523/2742
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SNAP- 170523/2743
Product: sn	apdragon_w5\+	_gen_1_w	earable_platform_firm	iware	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SNAP- 170523/2744
Product: sn	apdragon_wear_	_2100_pla	atform_firmware		
Affected Ver	sion(s): -				

0-1

1-2

2-33-44-5Page 1036 of 1106

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SNAP- 170523/2745
		_2500_pla	tform_firmware		
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SNAP- 170523/2746
Product: sn	apdragon_wear	_3100_pla	ntform_firmware		
Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SNAP- 170523/2747
Product: sn	apdragon_wear	_4100\+_]	platform_firmware	<u> </u>	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SNAP- 170523/2748
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://ww w.qualcomm	0-QUA-SNAP- 170523/2749

 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			
Memory after Effective Lifetime			accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	.com/compa ny/product- security/bull etins/may- 2023- bulletin				
Product: sn	apdragon_x12_l	te_moder	n_firmware					
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SNAP- 170523/2750			
Product: sn	Product: snapdragon_x20_lte_modem_firmware							
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SNAP- 170523/2751			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SNAP- 170523/2752			
Product: sn	apdragon_x24_l	te_moder	n_firmware					
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product-	O-QUA-SNAP- 170523/2753			

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SNAP- 170523/2754
Product: sn	apdragon_x50_5	g_moden	n-rf_system_firmware		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SNAP- 170523/2755
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SNAP- 170523/2756
Product: sn	apdragon_x55_5	g_moden	n-rf_system_firmware		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SNAP- 170523/2757

0-1

1-2

5-6

6-7

Missing Release of Memory after Effective Lifetime0.2-May-2023R.B.Memory Corruption in Graphics while accessing a buffer graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm com/compa ny/product. security/buil eins/may- 2023- builetin0.QUA-SNAP- 170523/2758Product: subjective Type Conversion or Cast0.2-May-2023R.B.Memory Corruption in Graphics while accessing a buffer (CVE ID : CVE-2023- 21666https://ww w.qualcomm com/compa ny/product security/buil eins/may- 2023- builetin0.QUA-SNAP- 170523/2758Incorrect Type Conversion or Cast0.2-May-2023R.B.Memory corruption in Graphics while accessing a buffer earcessing a buffer earcessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm com/compa ny/product security/buil eins/may- 2023-builetin0.QUA-SNAP- 170523/2759Missing Release of Release of after Effective Lifetime0.2-May-2023R.B.Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm com/compa ny/product security/buil eins/may- 2023- builetinMissing Release of after time0.2-May-2023R.B.Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 2023- builetinhttps://ww v.qualcomm com/compa ny/product security/buil eins/may- 2023-builetinMissing Release of corrects0.2-May-2023 <th>Weakness</th> <th>Publish Date</th> <th>CVSSv3</th> <th>Description &amp; CVE ID</th> <th>Patch</th> <th>NCIIPC ID</th>	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product. security/bull etins/may- 2023- bulletin0-QUA-SNAP- 170523/2759Missing Release of Memory after Effective Lifetime02-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-SNAP- 170523/2760Product: superstragon_x65_standard Type Conversion or Cast0.2-May-20237.8Memory corruption in Graphics while graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-SNAP- 170523/2760Product: superstragon_x65_standard Type Conversion or Cast0.2-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinProduct: superstragon_x65_standard Type Conversion or Cast0.2-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinProduct: superstragon_x65_standard Type0.2-May-20237.8Memory corruption in Graphics while importing a	Release of Memory after Effective	02-May-2023	7.8	in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b>	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-	÷
Incorrect Type Conversion or Cast0.2-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0QUA-SNAP- 170523/2759Missing Release of Memory after Effective Lifetime0.2-May-20237.8Memory Corruption in Graphics while alccated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0QUA-SNAP- 170523/2759Product: snape Supervise7.8Memory Corruption in Graphics while alccated through the 	Product: sn	apdragon_x5_lte	e_modem	firmware		
Incorrect Type Conversion or Cast0-9UA-SNAP- 170523/2759Incorrect Type Conversion or Cast0-9UA-SNAP- 170523/2759Missing Release of Memory after Effective Lifetime0-9UA-SNAP- 170523/27590-9UA-SNAP- 170523/27590-9UA-SNAP- 170523/2759Missing Release of Memory after Effective Lifetime0-9UA-SNAP- 170523/27590-9UA-SNAP- 170523/27590-9UA-SNAP- 170523/2760Product- Security/bull ether Lifetime0-9UA-SNAP- 170523/2760Product- Security/bull ether Lifetime0-9UA-SNAP- 170523/2760Incorrect Type Conversion or Cast7.8Memory corruption allocated through the graphics pool. CVE ID: CVE-2023- 21666https://ww w.qualcomm com/compa ny/product- security/bull etins/may- 2023- bulletinIncorrect Type Conversion or Cast7.8Memory corruption in Graphics while in Graphics whil	Affected Ver	sion(s): -				
Missing Release of Memory after Effective Lifetime02-May-20237.8Nemory of applics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-SNAP- 170523/2760Product: smap- security/bull etins/may- 2023- bulletinMemory corruption graphics pool. CVE ID : CVE-2023- 21666Nemory corruption nin Graphics while in Graphics wh	Type Conversion	02-May-2023	7.8	in Graphics while importing a file. <b>CVE ID : CVE-2023-</b>	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-	C C
Affected Version(s): -Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-SNAP- 170523/2761Product: snaphragon_xr1_ptform_firmware	Release of Memory after Effective	02-May-2023	7.8	in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b>	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-	-
Incorrect Type Conversion or Cast $ \begin{array}{c} 02-May-2023 \\ 02-May-2023 \end{array}, 7.8 \end{array} $ $ \begin{array}{c} Nemory corruption in Graphics while importing a file. \\ CVE ID: CVE-2023 \\ 21665 \end{array} $ $ \begin{array}{c} https://ww \\ w.qualcomm \\ ny/product- \\ security/bull \\ etins/may- \\ 2023- \\ bulletin \end{array} $ $ \begin{array}{c} 0-QUA-SNAP- \\ 170523/2761 \\ etins/may- \\ 2023- \\ bulletin \end{array} $	Product: sn	apdragon_x65_5	g_moden	n-rf_system_firmware		
Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-SNAP- 170523/2761Product: snaptragon_xr1_ptform_firmware	Affected Ver	sion(s): -	-		-	
	Type Conversion	02-May-2023	7.8	in Graphics while importing a file. <b>CVE ID : CVE-2023-</b>	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-	e
Affected Version(s): -	Product: sn	apdragon_xr1_p	latform_f	irmware		
	Affected Ver	sion(s): -				

0-1

1-2

2-3 3-4 4-5 Page **1040** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SNAP- 170523/2762
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SNAP- 170523/2763
Product: sn	apdragon_xr2\+	_gen_1_p	latform_firmware		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SNAP- 170523/2764
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SNAP- 170523/2765
Product: snapdragon_xr2_5g_platform_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull	O-QUA-SNAP- 170523/2766
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b> Page <b>1041</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
				etins/may- 2023- bulletin		
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SNAP- 170523/2767	
	m7250-aa_firmv	vare				
Affected Ver	sion(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SSM7- 170523/2768	
Product: sw	5100p_firmwar	е				
Affected Ver	sion(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SW51- 170523/2769	
Product: sw5100_firmware						
Affected Version(s): -						
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may-	0-QUA-SW51- 170523/2770	

0-1

1-2

2-3

3-4 4-5

5-6

6-7

Product: sxr1 Affected Versi				2023-	
				bulletin	
Affected Versi	1120_firmware				
	ion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SXR1- 170523/2771
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-SXR1- 170523/2772
Product: sxr2	2130_firmware				
Affected Versi	ion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SXR2- 170523/2773
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-SXR2- 170523/2774
Product: wcd	19326_firmwar	e			
Affected Versi	ion(s): -				

0-1

1-2

**2-3** 3-4 4-5 Page **1043** of **1106**  5-6

6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCD9- 170523/2775
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCD9- 170523/2776
Product: wo	d9330_firmwar	e			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-WCD9- 170523/2777
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCD9- 170523/2778
Product: wcd9335_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull	0-QUA-WCD9- 170523/2779
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10           Page 1044 of 1106					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
				etins/may- 2023- bulletin					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCD9- 170523/2780				
Product: wo	d9340_firmwar	е							
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCD9- 170523/2781				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCD9- 170523/2782				
Product: wo	d9341_firmwar	е							
Affected Ver	Affected Version(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-WCD9- 170523/2783				

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCD9- 170523/2784
	d9370_firmwar	e			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCD9- 170523/2785
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCD9- 170523/2786
Product: wo	d9371_firmwar	e		I	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCD9- 170523/2787
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	0-QUA-WCD9- 170523/2788

0-1

1-2

**2-3 3-4 4-5** Page **1046** of **1106**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin	
	d9375_firmwar	e			
Affected Ver	sion(s): -		Γ		
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-WCD9- 170523/2789
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCD9- 170523/2790
Product: wo	d9380_firmwar	e	L		
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCD9- 170523/2791
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCD9- 170523/2792
Product: wo	d9385_firmwar	e			

0-1

1-2

**2-3 3-4 4-5** Page **1047** of **1106**  5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCD9- 170523/2793
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCD9- 170523/2794
Product: wo	cn3610_firmwar	e			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2795
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2796
Product: wo	cn3615_firmwar	е			
Affected Ver	sion(s): -				
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product-	0-QUA-WCN3- 170523/2797
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5-6	6-7 7-8	<b>8 8-9 9-10</b>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Conversion or Cast			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2798				
Product: wo	m3620_firmwar	е							
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2799				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2800				
Product: wo	m3660b_firmwa	ire							
Affected Ver	Affected Version(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-WCN3- 170523/2801				

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2802
	n3660_firmwar	е			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2803
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2804
Product: wo	:n3680b_firmwa	ire			L
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2805
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	0-QUA-WCN3- 170523/2806

0-1

1-2

**2-3 3-4 4-5** Page **1050** of **1106**  8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin				
Product: wo	m3680_firmwar	e						
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2807			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2808			
Product: wo	m3910_firmwar	e						
Affected Ver	sion(s): -							
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2809			
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2810			
Product: wo	Product: wcn3950_firmware							

0-1

1-2

**2-3 3-4 4-5** Page **1051** of **1106**  5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): -	I			
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2811
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-WCN3- 170523/2812
Product: wo	cn3980_firmwar	е			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2813
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2814
Product: wo	cn3988_firmwar	e			
Affected Ver	sion(s): -				
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://ww w.qualcomm .com/compa ny/product-	0-QUA-WCN3- 170523/2815
CVSS Scoring S	Scale 0-1	1-2 2-3	<b>3-4 4-5 5-6</b>	6-7 7-8	<u> </u>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID				
Conversion or Cast			CVE ID : CVE-2023- 21665	security/bull etins/may- 2023- bulletin					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2816				
Product: wo	m3990_firmwar	e							
Affected Ver	sion(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN3- 170523/2817				
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-WCN3- 170523/2818				
Product: wo	m3998_firmwar	e							
Affected Ver	Affected Version(s): -								
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-WCN3- 170523/2819				

0-1

1-2

5-6

6-7

Missing Release of Memory after Effective Lifetime0.2-May-20237.8Memory Corruption in Graphics while accessing a buffer graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm com/compa ny/product- security/buil etins/may- 202.3 builetin0-QUA-WCN3- 170523/2820Product: wersongsp. firmwareMemory Corruption in Graphics while accessing a buffer graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm com/compa ny/product- security/buil etins/may- 202-May-20230-QUA-WCN3- 170523/2821Incorrect Type Conversion or Cast0.2-May-20237.8Memory corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21665https://ww w.qualcomm com/compa ny/product- security/buil etins/may- 2023- builetin0-QUA-WCN3- 170523/2821Missing Release of Memory after Effective Lifetime7.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm com/compa ny/product- security/buil etins/may- 2023- builetinProduct: Wemory after Effective Lifetime0.2-May-2023 2-May-20237.8Memory corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm com/compa ny/product- security/buil etins/may- 2023- builetinProduct: Type Conversion or Cast0.2-May-2023 2-May-20237.8Memory corruptio	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
Affected Version(s): -Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-WCN3- 170523/2821Missing Release of Memory after Effective Lifetime02-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-WCN3- 170523/2822Product: wcorrect Type Conversion or Cast0.2-May-20237.8Memory corruption in Graphics while graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-WCN3- 170523/2822Product: wcorrect Type Conversion or Cast0.2-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinProduct: wcorrect Type Conversion or Cast0.2-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletinProduct: wcorrect Type0.2-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qual	Release of Memory after Effective	02-May-2023	7.8	in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b>	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-	•	
Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-WCN3- 170523/2821Missing Release of Memory after Effective Lifetime02-May-20237.8Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-WCN3- 170523/2822Product: wc-740_firmware Type Conversion 	Product: wo	m3999_firmwar	е				
Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665w.qualcomm com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-WCN3- 170523/2821Missing Release of Memory after Effective Lifetime0-2-May-2023F.84Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-WCN3- 170523/2822Product: version7.8Memory corruption in Graphics while arghics pool. CVE ID : CVE-2023- 21666https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-WCN3- 170523/2822Product: version0-2-May-20237.8Memory corruption in Graphics while in Graphics whi	Affected Vers	sion(s): -					
Missing Release of Memory after Effective Lifetime02-May-20237.8Nemory radicated through the graphics pool. CVE ID : CVE-2023- 21666w.qualcomm r.com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-WCN3- 170523/2822 <b>Product: wcorototototototototototototototototototo</b>	Type Conversion	02-May-2023	7.8	in Graphics while importing a file. <b>CVE ID : CVE-2023-</b>	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-	÷	
Affected Version(s): -Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b> https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-WCN6- 170523/2823Product: wcroto_firmware7.8Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> bulletin0-QUA-WCN6- 170523/2823	Release of Memory after Effective	02-May-2023	7.8	in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b>	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-	÷	
Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b> https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-WCN6- 170523/2823Product: wcn6750_firmwareVVImage: Compa mark Distribution of the security of the sec	Product: wc	m6740_firmwar	e				
Incorrect Type Conversion or Cast02-May-20237.8Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665w.qualcomm .om/compa ny/product- security/bull etins/may- 2023- bulletin0-QUA-WCN6- 170523/2823Product: wcr6750_firmware	Affected Vers	sion(s): -					
	Type Conversion	02-May-2023	7.8	in Graphics while importing a file. <b>CVE ID : CVE-2023-</b>	w.qualcomm .com/compa ny/product- security/bull etins/may- 2023-	C C	
Affected Version(s): -	Product: wcn6750_firmware						
	Affected Vers	sion(s): -					

0-1

1-2

**2-3 3-4 4-5** Page **1054** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN6- 170523/2824
Product: wo	cn685x-1_firmw	are			
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	O-QUA-WCN6- 170523/2825
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN6- 170523/2826
Product: wo	m685x-5_firmw	are		I	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WCN6- 170523/2827
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://ww w.qualcomm .com/compa ny/product- security/bull	0-QUA-WCN6- 170523/2828

0-1

1-2

**2-3 3-4 4-5** Page **1055** of **1106**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			CVE ID : CVE-2023- 21666	etins/may- 2023- bulletin	
Product: ws	a8810_firmwar	е			
Affected Ver	sion(s): -				-
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WSA8- 170523/2829
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WSA8- 170523/2830
Product: ws	a8815_firmwar	е		I	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. <b>CVE ID : CVE-2023-</b> <b>21665</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WSA8- 170523/2831
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. <b>CVE ID : CVE-2023-</b> <b>21666</b>	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WSA8- 170523/2832
Product: ws	a8830_firmwar	е			1

0-1

1-2

**2-3 3-4 4-5** Page **1056** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): -		L		L
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WSA8- 170523/2833
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WSA8- 170523/2834
Product: ws	a8835_firmwar	е		I	
Affected Ver	sion(s): -				
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. CVE ID : CVE-2023- 21665	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WSA8- 170523/2835
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. CVE ID : CVE-2023- 21666	https://ww w.qualcomm .com/compa ny/product- security/bull etins/may- 2023- bulletin	0-QUA-WSA8- 170523/2836
Vendor: Red	dhat				
Product: en	terprise_linux				
Affected Ver	sion(s): 6.0				
Use After Free	08-May-2023	6.7	A use-after-free vulnerability was	https://githu b.com/torval	O-RED-ENTE- 170523/2837

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	Dago 1057 of 1106									

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			found in the Linux kernel's ext4 filesystem in the way it handled the extra inode size for extended attributes. This flaw could allow a privileged local user to cause a system crash or other undefined behaviors.	ds/linux/co mmit/67d7d 8ad99be	
			CVE ID : CVE-2023- 2513		
Affected Ver	sion(s): 7.0				
Use After Free	08-May-2023	7.8	In the Linux kernel through 6.3.1, a use- after-free in Netfilter nf_tables when processing batch requests can be abused to perform arbitrary read and write operations on kernel memory. Unprivileged local users can obtain root privileges. This occurs because anonymous sets are mishandled. <b>CVE ID : CVE-2023- 32233</b>	https://githu b.com/torval ds/linux/co mmit/c1592 a89942e967 8f7d9c8030e fa777c0d57e dab, https://git.k ernel.org/cgi t/linux/kern el/git/torval ds/linux.git/ commit/?id= c1592a8994 2e9678f7d9c 8030efa777c 0d57edab	O-RED-ENTE- 170523/2838
Use After Free	08-May-2023	6.7	A use-after-free vulnerability was found in the Linux kernel's ext4 filesystem in the way it handled the extra inode size for extended attributes. This flaw could allow	https://githu b.com/torval ds/linux/co mmit/67d7d 8ad99be	O-RED-ENTE- 170523/2839

0-1

1-2

**2-3 3-4 4-5** Page **1058** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a privileged local user to cause a system crash or other undefined behaviors.		
			CVE ID : CVE-2023- 2513		
Affected Ver	sion(s): 8.0				
Use After Free	08-May-2023	7.8	In the Linux kernel through 6.3.1, a use- after-free in Netfilter nf_tables when processing batch requests can be abused to perform arbitrary read and write operations on kernel memory. Unprivileged local users can obtain root privileges. This occurs because anonymous sets are mishandled. <b>CVE ID : CVE-2023- 32233</b>	https://githu b.com/torval ds/linux/co mmit/c1592 a89942e967 8f7d9c8030e fa777c0d57e dab, https://git.k ernel.org/cgi t/linux/kern el/git/torval ds/linux.git/ commit/?id= c1592a8994 2e9678f7d9c 8030efa777c 0d57edab	O-RED-ENTE- 170523/2840
Use After Free	08-May-2023	6.7	A use-after-free vulnerability was found in the Linux kernel's ext4 filesystem in the way it handled the extra inode size for extended attributes. This flaw could allow a privileged local user to cause a system crash or other undefined behaviors. <b>CVE ID : CVE-2023- 2513</b>	https://githu b.com/torval ds/linux/co mmit/67d7d 8ad99be	O-RED-ENTE- 170523/2841

0-1

1-2

**2-3 3-4 4-5** Page **1059** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Ver	sion(s): 9.0				
Use After Free	08-May-2023	7.8	In the Linux kernel through 6.3.1, a use- after-free in Netfilter nf_tables when processing batch requests can be abused to perform arbitrary read and write operations on kernel memory. Unprivileged local users can obtain root privileges. This occurs because anonymous sets are mishandled. <b>CVE ID : CVE-2023- 32233</b>	https://githu b.com/torval ds/linux/co mmit/c1592 a89942e967 8f7d9c8030e fa777c0d57e dab, https://git.k ernel.org/cgi t/linux/kern el/git/torval ds/linux.git/ commit/?id= c1592a8994 2e9678f7d9c 8030efa777c 0d57edab	O-RED-ENTE- 170523/2842
Use After Free	08-May-2023	6.7	A use-after-free vulnerability was found in the Linux kernel's ext4 filesystem in the way it handled the extra inode size for extended attributes. This flaw could allow a privileged local user to cause a system crash or other undefined behaviors. <b>CVE ID : CVE-2023- 2513</b>	https://githu b.com/torval ds/linux/co mmit/67d7d 8ad99be	O-RED-ENTE- 170523/2843
Vendor: Ro	ckwellautomatio	on			
Product: armorstart_st_281e_firmware					
Affected Ver	sion(s): -				
Improper Neutralizat ion of	11-May-2023	7.1	A cross site scripting vulnerability was	https://rock wellautomati on.custhelp.c	O-ROC-ARMO- 170523/2844
CVSS Scoring S	Scale 0-1	L-2 2-3	3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1060 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.	om/app/ans wers/answe r_view/a_id/ 1139438	
			CVE ID : CVE-2023- 29030		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	7.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	O-ROC-ARMO- 170523/2845

0-1

1-2

**2-3 3-4 4-5** Page **1061** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29031		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	6.5	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product A cross site scripting vulnerability was discovered that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	O-ROC-ARMO- 170523/2846
Improper Neutralizat			<b>CVE ID : CVE-2023- 29024</b> A cross site scripting	https://rock wellautomati	
ion of Input During Web Page Generation	11-May-2023	6.1	vulnerability was discovered in Rockwell Automation's ArmorStart ST	on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	0-ROC-ARMO- 170523/2847

0-1

1-2

2-3 3-4 4-5 Page 1062 of 1106 5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.		
			CVE ID : CVE-2023- 29023		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	O-ROC-ARMO- 170523/2848

0-1

1-2

**2-3 3-4 4-5** Page **1063** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29022		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	0-ROC-ARMO- 170523/2849
			CVE ID : CVE-2023- 29025		
Improper Neutralizat ion of Input During Web Page	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell	https://rock wellautomati on.custhelp.c om/app/ans wers/answe	O-ROC-ARMO- 170523/2850

0-1

1-2

**2-3 3-4 4-5** Page **1064** of **1106**  8-9

9-10

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Automation's ArmorStart ST product	r_view/a_id/ 1139438	
			that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.		
			29026		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	O-ROC-ARMO- 170523/2851

0-1

1-2

**2-3 3-4 4-5** Page **1065** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.		
			CVE ID : CVE-2023- 29027		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	O-ROC-ARMO- 170523/2852

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29028		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	0-ROC-ARMO- 170523/2853
			CVE ID : CVE-2023- 29029		
	morstart_st_284	ee_firmw	vare		
Affected Version(s): -					
Improper Neutralizat ion of Input During Web Page	11-May-2023	7.1	A cross site scripting vulnerability was discovered in Rockwell	https://rock wellautomati on.custhelp.c om/app/ans wers/answe	O-ROC-ARMO- 170523/2854
CVSS Scoring S	Scale 0-1	1-2 2-3	3-4 4-5 5-6 Page <b>1067</b> of <b>1106</b>	6-7 7-8	8 8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.	r_view/a_id/ 1139438	
			CVE ID : CVE-2023- 29030		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	7.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	0-ROC-ARMO- 170523/2855

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29031		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	6.5	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product A cross site scripting vulnerability was discovered that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	0-ROC-ARMO- 170523/2856
			CVE ID : CVE-2023- 29024		
Improper Neutralizat ion of Input During Web Page Generation	11-May-2023	6.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	O-ROC-ARMO- 170523/2857

0-1

1-2

**2-3 3-4 4-5** Page **1069** of **1106**  5-6

6-7

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.		
			CVE ID : CVE-2023- 29023		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	0-ROC-ARMO- 170523/2858

0-1

1-2

**2-3 3-4 4-5** Page **1070** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29022		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	O-ROC-ARMO- 170523/2859
Improper Neutralizat ion of Input During Web Page Generation	11-May-2023	5.9	29025 A cross site scripting vulnerability was discovered in Rockwell Automation's	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	O-ROC-ARMO- 170523/2860
CVSS Scoring S	Scale 0-1 2	1-2 2-3	<b>3-44-55-6</b> Page <b>1071</b> of <b>1106</b>	6-7 7-8	8 8-9 9-10

Page 1071 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			ArmorStart ST product		
			that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.		
			CVE ID : CVE-2023- 29026		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface.	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	O-ROC-ARMO- 170523/2861

0-1

1-2

2-3 3-4 4-5 Page **1072** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Additionally, a malicious user could potentially cause interruptions to the availability of the web page.		
			CVE ID : CVE-2023- 29027		
			A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	0-ROC-ARMO- 170523/2862

0-1

1-2

2-3 3-4 4-5 Page **1073** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29028		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. <b>CVE ID : CVE-2023- 29029</b>	https://rock wellautomati on.custhelp.c om/app/ans wers/answe r_view/a_id/ 1139438	0-ROC-ARMO- 170523/2863
Vendor: San	nsung				
Product: an	_				
Affected Vers	sion(s): 11.0				
Buffer Copy without Checking Size of Input	04-May-2023	9.8	Potential buffer overflow vulnerability in mm_Plmncoordinati on.c in Shannon baseband prior to	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea	O-SAM-ANDR- 170523/2864
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
('Classic Buffer Overflow')			SMR May-2023 Release 1 allows remote attackers to cause invalid memory access.	r=2023&mo nth=05	
			CVE ID : CVE-2023- 21504		
Improper Authentica tion	04-May-2023	7.8	Improper access control vulnerability in AppLock prior to SMR May-2023 Release 1 allows local attackers without proper permission to execute a privileged operation. <b>CVE ID : CVE-2023-</b> <b>21484</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2865
N/A	04-May-2023	7.8	Improper access control vulnerablility in Tips prior to SMR May-2023 Release 1 allows local attackers to launch arbitrary activity in Tips. <b>CVE ID : CVE-2023-</b> <b>21488</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2866
N/A	04-May-2023	7.1	Improper access control in GearManagerStub prior to SMR May- 2023 Release 1 allows a local attacker to delete applications installed by watchmanager. <b>CVE ID : CVE-2023-</b> <b>21490</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2867

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	04-May-2023	6.8	Heap out-of-bounds write vulnerability in bootloader prior to SMR May-2023 Release 1 allows a physical attacker to execute arbitrary code. <b>CVE ID : CVE-2023-</b> <b>21489</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2868
N/A	04-May-2023	5.5	Improper access control vulnerability in SemShareFileProvid er prior to SMR May- 2023 Release 1 allows local attackers to access protected data. <b>CVE ID : CVE-2023-</b> <b>21493</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2869
N/A	04-May-2023	5.5	Improper access control vulnerability in Knox Enrollment Service prior to SMR May-2023 Release 1 allow attacker install KSP app when device admin is set. <b>CVE ID : CVE-2023-</b> <b>21495</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2870
N/A	04-May-2023	5.5	Active Debug Code vulnerability in ActivityManagerServ ice prior to SMR May-2023 Release 1 allows attacker to use debug function via setting debug level.	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2871

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21496		
N/A	04-May-2023	4.6	Improper export of android application components vulnerability in VideoPreviewActivit y in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox. <b>CVE ID : CVE-2023-</b> <b>21485</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2872
N/A	04-May-2023	4.6	Improper export of android application components vulnerability in ImagePreviewActivit y in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox. <b>CVE ID : CVE-2023-</b> <b>21486</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2873
Insertion of Sensitive Informatio n into Log File	04-May-2023	4.4	Kernel pointers are printed in the log file prior to SMR May- 2023 Release 1 allows a privileged local attacker to bypass ASLR. <b>CVE ID : CVE-2023-</b> <b>21492</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2874

0-1

1-2

**2-3 3-4 4-5** Page **1077** of **1106**  6-7 7-8

5-6

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentica tion	04-May-2023	3.3	Improper access control vulnerability in Telephony framework prior to SMR May-2023 Release 1 allows local attackers to change a call setting. <b>CVE ID : CVE-2023-</b> <b>21487</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2875
Affected Ver	sion(s): 12.0				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-May-2023	9.8	Potential buffer overflow vulnerability in mm_Plmncoordinati on.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access. <b>CVE ID : CVE-2023-</b> <b>21504</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2876
Improper Authentica tion	04-May-2023	7.8	Improper access control vulnerability in AppLock prior to SMR May-2023 Release 1 allows local attackers without proper permission to execute a privileged operation. <b>CVE ID : CVE-2023-</b> <b>21484</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2877
N/A	04-May-2023	7.8	Improper access control vulnerablility in Tips prior to SMR May-2023 Release 1 allows local attackers to launch	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea	O-SAM-ANDR- 170523/2878

0-1

1-2

**2-3 3-4 4-5** Page **1078** of **1106**  8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary activity in Tips. <b>CVE ID : CVE-2023-</b>	r=2023&mo nth=05	
			21488		
N/A	04-May-2023	7.8	Improper access control vulnerability in ThemeManager prior to SMR May- 2023 Release 1 allows local attackers to write arbitrary files with system privilege.	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2879
			CVE ID : CVE-2023- 21491		
Improper Input Validation	04-May-2023	7.8	Improper input validation vulnerability in FactoryTest application prior to SMR May-2023 Release 1 allows local attackers to get privilege escalation via debugging commands. <b>CVE ID : CVE-2023-</b> <b>21502</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2880
N/A	04-May-2023	7.1	Improper access control in GearManagerStub prior to SMR May- 2023 Release 1 allows a local attacker to delete applications installed by watchmanager. <b>CVE ID : CVE-2023-</b> <b>21490</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2881

0-1

1-2

**2-3 3-4 4-5** Page **1079** of **1106**  5-6

6-7 7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	04-May-2023	6.8	Heap out-of-bounds write vulnerability in bootloader prior to SMR May-2023 Release 1 allows a physical attacker to execute arbitrary code. <b>CVE ID : CVE-2023-</b> <b>21489</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2882
N/A	04-May-2023	5.5	Improper access control vulnerability in SemShareFileProvid er prior to SMR May- 2023 Release 1 allows local attackers to access protected data. <b>CVE ID : CVE-2023-</b> <b>21493</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2883
N/A	04-May-2023	5.5	Improper access control vulnerability in Knox Enrollment Service prior to SMR May-2023 Release 1 allow attacker install KSP app when device admin is set. <b>CVE ID : CVE-2023-</b> <b>21495</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2884
N/A	04-May-2023	5.5	Active Debug Code vulnerability in ActivityManagerServ ice prior to SMR May-2023 Release 1 allows attacker to use debug function via setting debug level.	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2885

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21496		
N/A	04-May-2023	4.6	Improper export of android application components vulnerability in VideoPreviewActivit y in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox. <b>CVE ID : CVE-2023-</b> <b>21485</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2886
N/A	04-May-2023	4.6	Improper export of android application components vulnerability in ImagePreviewActivit y in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox. <b>CVE ID : CVE-2023-</b> <b>21486</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2887
Insertion of Sensitive Informatio n into Log File	04-May-2023	4.4	Kernel pointers are printed in the log file prior to SMR May- 2023 Release 1 allows a privileged local attacker to bypass ASLR. <b>CVE ID : CVE-2023-</b> <b>21492</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2888

0-1

1-2

**2-3 3-4 4-5** Page **1081** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentica tion	04-May-2023	3.3	Improper access control vulnerability in Telephony framework prior to SMR May-2023 Release 1 allows local attackers to change a call setting. <b>CVE ID : CVE-2023-</b> <b>21487</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2889
Affected Ver	sion(s): 13.0				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-May-2023	9.8	Potential buffer overflow vulnerability in auth api in mm_Authentication.c in Shannon baseband prior to SMR May- 2023 Release 1 allows remote attackers to cause invalid memory access. <b>CVE ID : CVE-2023-</b> 21494	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2890
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-May-2023	9.8	Potential buffer overflow vulnerability in mm_LteInterRatMan agement.c in Shannon baseband prior to SMR May- 2023 Release 1 allows remote attackers to cause invalid memory access. <b>CVE ID : CVE-2023-</b> <b>21503</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2891
Buffer Copy without	04-May-2023	9.8	Potential buffer overflow vulnerability in	https://secu rity.samsung mobile.com/	O-SAM-ANDR- 170523/2892

0-1

1-2

**2-3 3-4 4-5** Page **1082** of **1106**  6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			mm_Plmncoordinati on.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access. <b>CVE ID : CVE-2023-</b>	securityUpd ate.smsb?yea r=2023&mo nth=05	
			21504		
Improper Authentica tion	04-May-2023	7.8	Improper access control vulnerability in AppLock prior to SMR May-2023 Release 1 allows local attackers without proper permission to execute a privileged operation. <b>CVE ID : CVE-2023-</b> <b>21484</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2893
N/A	04-May-2023	7.8	Improper access control vulnerablility in Tips prior to SMR May-2023 Release 1 allows local attackers to launch arbitrary activity in Tips. <b>CVE ID : CVE-2023-</b> <b>21488</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2894
N/A	04-May-2023	7.8	Improper access control vulnerability in ThemeManager prior to SMR May- 2023 Release 1 allows local attackers to write arbitrary files with system privilege.	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2895

0-1

1-2

**2-3 3-4 4-5** Page **1083** of **1106**  5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21491		
Use of Externally- Controlled Format String	04-May-2023	7.8	Use of externally- controlled format string vulnerability in mPOS TUI trustlet prior to SMR May- 2023 Release 1 allows local attackers to access the memory address. <b>CVE ID : CVE-2023-</b> <b>21497</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2896
Improper Input Validation	04-May-2023	7.8	Improper input validation vulnerability in setPartnerTAInfo in mPOS TUI trustlet prior to SMR May- 2023 Release 1 allows local attackers to overwrite the trustlet memory. <b>CVE ID : CVE-2023-</b> <b>21498</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2897
Out-of- bounds Write	04-May-2023	7.8	Out-of-bounds write vulnerability in TA_Communication_ mpos_encrypt_pin in mPOS TUI trustlet prior to SMR May- 2023 Release 1 allows local attackers to execute arbitrary code. <b>CVE ID : CVE-2023-</b> 21499	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2898
Improper Input Validation	04-May-2023	7.8	Improper input validation vulnerability in mPOS fiserve trustlet	https://secu rity.samsung mobile.com/ securityUpd	O-SAM-ANDR- 170523/2899

0-1

1-2

**2-3** 3-4 4-5 Page **1084** of **1106**  8-9

9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to SMR May- 2023 Release 1 allows local attackers to execute arbitrary code.	ate.smsb?yea r=2023&mo nth=05	
			CVE ID : CVE-2023- 21501		
Improper Input Validation	04-May-2023	7.8	Improper input validation vulnerability in FactoryTest application prior to SMR May-2023 Release 1 allows local attackers to get privilege escalation via debugging commands.	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2900
			CVE ID : CVE-2023- 21502		
N/A	04-May-2023	7.1	Improper access control in GearManagerStub prior to SMR May- 2023 Release 1 allows a local attacker to delete applications installed by watchmanager. <b>CVE ID : CVE-2023-</b> <b>21490</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2901
Out-of- bounds Write	04-May-2023	6.8	Heap out-of-bounds write vulnerability in bootloader prior to SMR May-2023 Release 1 allows a physical attacker to execute arbitrary code. <b>CVE ID : CVE-2023-</b> <b>21489</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2902

0-1

1-2

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-May-2023	5.5	Improper access control vulnerability in SemShareFileProvid er prior to SMR May- 2023 Release 1 allows local attackers to access protected data. <b>CVE ID : CVE-2023-</b> <b>21493</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2903
N/A	04-May-2023	5.5	Improper access control vulnerability in Knox Enrollment Service prior to SMR May-2023 Release 1 allow attacker install KSP app when device admin is set. <b>CVE ID : CVE-2023-</b> <b>21495</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2904
N/A	04-May-2023	5.5	Active Debug Code vulnerability in ActivityManagerServ ice prior to SMR May-2023 Release 1 allows attacker to use debug function via setting debug level. <b>CVE ID : CVE-2023- 21496</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2905
Double Free	04-May-2023	5.5	Double free validation vulnerability in setPinPadImages in mPOS TUI trustlet prior to SMR May- 2023 Release 1 allows local attackers to access the trustlet memory.	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2906

0-1

1-2

**2-3 3-4 4-5** Page **1086** of **1106**  5-6

6-7

7-8 8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 21500		
N/A	04-May-2023	4.6	Improper export of android application components vulnerability in VideoPreviewActivit y in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox. <b>CVE ID : CVE-2023-</b> <b>21485</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2907
N/A	04-May-2023	4.6	Improper export of android application components vulnerability in ImagePreviewActivit y in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox. <b>CVE ID : CVE-2023-</b> <b>21486</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2908
Insertion of Sensitive Informatio n into Log File	04-May-2023	4.4	Kernel pointers are printed in the log file prior to SMR May- 2023 Release 1 allows a privileged local attacker to bypass ASLR. <b>CVE ID : CVE-2023-</b> <b>21492</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	0-SAM-ANDR- 170523/2909

0-1

1-2

**2-3 3-4 4-5** Page **1087** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentica tion	04-May-2023	3.3	Improper access control vulnerability in Telephony framework prior to SMR May-2023 Release 1 allows local attackers to change a call setting. <b>CVE ID : CVE-2023-</b> <b>21487</b>	https://secu rity.samsung mobile.com/ securityUpd ate.smsb?yea r=2023&mo nth=05	O-SAM-ANDR- 170523/2910
Product: ex	ynos_1080_firm	ware			
Affected Ver	sion(s): -				
Improper Handling of Exceptiona l Conditions	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface. <b>CVE ID : CVE-2023- 29092</b>	https://semi conductor.sa msung.com/ support/qua lity- support/pro duct- security- updates/	O-SAM-EXYN- 170523/2911
	ynos_5123_firm	ware			
Affected Ver	sion(s): -				
Improper Handling of Exceptiona l Conditions	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, and Exynos 1080.	https://semi conductor.sa msung.com/ support/qua lity- support/pro duct- security- updates/	O-SAM-EXYN- 170523/2912

1-2

**2-3** 3-4 4-5 Page **1088** of **1106**  5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface.		
			CVE ID : CVE-2023- 29092		
Product: ex	ynos_5300_firm	ware			
Affected Ver	sion(s): -				
Improper Handling of Exceptiona l Conditions	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface. <b>CVE ID : CVE-2023-</b>	https://semi conductor.sa msung.com/ support/qua lity- support/pro duct- security- updates/	O-SAM-EXYN- 170523/2913
Product: ex	ynos_980_firmw	are	29092		
Affected Ver	-				
Improper Handling of Exceptiona l Conditions	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong	https://semi conductor.sa msung.com/ support/qua lity- support/pro duct- security- updates/	O-SAM-EXYN- 170523/2914

0-1

1-2

5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resource can occur due to improper handling of parameters while binding a network interface. <b>CVE ID : CVE-2023-</b>		
			29092		
Vendor: sha	apeshift				I
Product: ke	epkey_firmware	e			
Affected Ver	sion(s): From (in	cluding) 7	7.5.2 Up to (excluding) 7	.7.0	
Out-of- bounds Read	02-May-2023	5.7	Insufficient length checks in the ShapeShift KeepKey hardware wallet firmware before 7.7.0 allow a global buffer overflow via crafted messages. Flaws in cf_confirmExecTx() in ethereum_contracts. c can be used to reveal arbitrary microcontroller memory on the device screen or crash the device. With physical access to a PIN-unlocked device, attackers can extract the BIP39 mnemonic secret from the hardware wallet. <b>CVE ID : CVE-2023- 27892</b>	https://githu b.com/keepk ey/keepkey- firmware/pu ll/337	O-SHA-KEEP- 170523/2915
Vendor: Sie					
	sion(s): * Up to (		) 2.1		
			3-4 4-5 5-6		
CVSS Scoring	Scale 0-1	1-2 2-3	<b>3 3-4 4-5 5-6</b> Page <b>1090</b> of <b>1106</b>	6-7 7-8	8 8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Standardiz ed Error Handling Mechanism	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device is vulnerable to a denial of service while parsing a random (non-JSON) MQTT payload. This could allow an attacker who can manipulate the communication between the MQTT broker and the affected device to cause a denial of service (DoS). <b>CVE ID : CVE-2023- 29105</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	0-SIE-6GK1- 170523/2916
Use of Hard- coded Password	09-May-2023	4.3	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	O-SIE-6GK1- 170523/2917

0-1

1-2

**2-3 3-4 4-5** Page **1091** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device uses a hard-coded password to protect the diagnostic files. This could allow an authenticated attacker to access protected data.		
			CVE ID : CVE-2023- 29103		
Affected Ver	rsion(s): 2.0				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	7.6	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to overwrite any file the Linux user `ccuser` has write access to, or to download any file the Linux user `ccuser` has read- only access to.	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	O-SIE-6GK1- 170523/2918

0-1

1-2

**2-3 3-4 4-5** Page **1092** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023- 29104		
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint is accessible via REST API without authentication. This could allow an unauthenticated remote attacker to download the files available via the endpoint. <b>CVE ID : CVE-2023- 29106</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	O-SIE-6GK1- 170523/2919
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	09-May-2023	7.2	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The web based management of affected devices does not properly validate user input, making it susceptible to command injection. This could allow an authenticated privileged remote attacker to execute	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	O-SIE-6GK1- 170523/2920

0-1

1-2

**2-3** 3-4 4-5 Page **1093** of **1106**  6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root privileges. <b>CVE ID : CVE-2023-</b>		
			28832		
Files or Directories Accessible to External Parties	09-May-2023	5.3	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint discloses some undocumented files. This could allow an unauthenticated remote attacker to gain access to additional information resources. <b>CVE ID : CVE-2023- 29107</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	O-SIE-6GK1- 170523/2921
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	2.7	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	O-SIE-6GK1- 170523/2922

0-1

1-2

**2-3** 3-4 4-5 Page **1094** of **1106**  6-7 7-8

5-6

8-9 9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated privileged remote attacker to write any file with the extension `.db`.		
			CVE ID : CVE-2023- 29128		
Product: 6g	k1411-5ac00_fi	rmware			
Affected Ver	sion(s): * Up to (e	excluding)	2.1		
Missing Standardiz ed Error Handling Mechanism	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device is vulnerable to a denial of service while parsing a random (non-JSON) MQTT payload. This could allow an attacker who can manipulate the communication between the MQTT broker and the affected device to cause a denial of service (DoS). <b>CVE ID : CVE-2023- 29105</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	O-SIE-6GK1- 170523/2923

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard- coded Password	09-May-2023	4.3	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device uses a hard-coded password to protect the diagnostic files. This could allow an authenticated attacker to access protected data. <b>CVE ID : CVE-2023- 29103</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	O-SIE-6GK1- 170523/2924
Affected Ver	sion(s): 2.0				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	7.6	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	O-SIE-6GK1- 170523/2925

0-1

1-2

**2-3 3-4 4-5** Page **1096** of **1106**  5-6

6-7

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated privileged remote attacker to overwrite any file the Linux user `ccuser` has write access to, or to download any file the Linux user `ccuser` has read- only access to. <b>CVE ID : CVE-2023-</b> <b>29104</b>		
Exposure of Sensitive Informatio n to an Unauthoriz ed Actor	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint is accessible via REST API without authentication. This could allow an unauthenticated remote attacker to download the files available via the endpoint. <b>CVE ID : CVE-2023-</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	O-SIE-6GK1- 170523/2926
Improper Neutralizat ion of Special Elements used in a Command ('Comman	09-May-2023	7.2	29106 A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	O-SIE-6GK1- 170523/2927

0-1

1-2

**2-3 3-4 4-5** Page **1097** of **1106**  5-6

6-7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			web based management of affected devices does not properly validate user input, making it susceptible to command injection. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges. <b>CVE ID : CVE-2023- 28832</b>		
Files or Directories Accessible to External Parties	09-May-2023	5.3	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint discloses some undocumented files. This could allow an unauthenticated remote attacker to gain access to additional information resources. <b>CVE ID : CVE-2023- 29107</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	O-SIE-6GK1- 170523/2928
Improper Limitation of a Pathname to a Restricted Directory	09-May-2023	2.7	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 555292.pdf	O-SIE-6GK1- 170523/2929

0-1

1-2

**2-3** 3-4 4-5 Page **1098** of **1106** 

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to write any file with the extension `.db`. CVE ID : CVE-2023- 29128		
Product: sca	alance_lpe9403_	firmware	5		
Affected Ver	sion(s): * Up to (	excluding)	2.1		
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	09-May-2023	9.9	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). The web based management of affected device does not properly validate user input, making it susceptible to command injection. This could allow an authenticated remote attacker to access the underlying operating system as the root user. <b>CVE ID : CVE-2023- 27407</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 325383.pdf	O-SIE-SCAL- 170523/2930
Creation of Temporary	09-May-2023	3.3	A vulnerability has been identified in	https://cert- portal.sieme	0-SIE-SCAL- 170523/2931

0-1

1-2

3-4 4-5 2-3 Page 1099 of 1106 6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File With Insecure Permission s			SCALANCE LPE9403 (All versions < V2.1). The `i2c` mutex file is created with the permissions bits of `- rw-rw-rw-`. This file is used as a mutex for multiple applications interacting with i2c. This could allow an authenticated attacker with access to the SSH interface on the affected device to interfere with the integrity of the mutex and the data it protects. <b>CVE ID : CVE-2023- 27408</b>	ns.com/prod uctcert/pdf/ ssa- 325383.pdf	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	3.3	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). A path traversal vulnerability was found in the `deviceinfo` binary via the `mac` parameter. This could allow an authenticated attacker with access to the SSH interface on the affected device to read the contents of any file named `address`. <b>CVE ID : CVE-2023- 27409</b>	https://cert- portal.sieme ns.com/prod uctcert/pdf/ ssa- 325383.pdf	O-SIE-SCAL- 170523/2932

0-1

1-2

2-33-44-5Page 1100 of 1106

6-7 7-8

5-6

9-10

Heap- based Buffer Overflow       09-May-2023       A vulnerability has been identified in SCALANCE LPS403 (All versions < V2.1). A heap-based buffer overflow       https://cert- portal.steme routerity was found in the 'edgebox.web.app' binary. The binary with a backup password longer than 255 characters. This could allow an authenticated privileged attacker to cause a denial of service.       0-SIE-SCAL- 170523/2933         Vendor: spryker       Vertifield Privileged attacker to cause a denial of service.       0-SIE-SCAL- 170523/2933         Metap-based buffer overflow       0-May-2023       SQL Privileged attacker to cause a denial of service.       0-SIE-SCAL- 170523/2934         Vendor: spryker       Vertorized Privileged attacker to cause a denial of service.       0-SIE-SCAL- 170523/2934         Metap-based buffer overflow       04-May-2023       SQL injection vulnerability inSpryker Commerce OS 0.9 that allows for access to sensitive data via customer/order?ord erSearchForm[search hText]=       N/A       0-SPR-COMM- 170523/2934         Vendor: Teruda       VEI ID: CVE-2023- 27568       Vertorized Privileged attacker       N/A       0-SPR-COMM- 170523/2934         Vendor: Teruda       SQL (SQL Injection)       0-TEN-AC18- 170523/2933       0-TEN-AC18- 170523/2934         Vendor: Teruda       0-SMay-2023       9.8       Tenda AC18 v15.03.05.19(518.1) _cn was discovered       https://githu bcom/Drizzl ingSun/Tend       0-TEN-AC18- 170523/2935	Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID		
Product: commerce_os         Affected Version(s): 0.9         Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')       SQL injection vulnerability inSpryker Commerce OS 0.9 that allows for access to sensitive data via customer/order?ord erSearchForm[searc hText]= CVE ID : CVE-2023- 27568       N/A       0-SPR-COMM- 170523/2934         Vendor: Temtation       E       E       CVE ID : CVE-2023- 27568       N/A       0-SPR-COMM- 170523/2934         Vendor: Temtation         Froduct: act=firmware         Tenda AC18 v15.03.05.19(6318_) _cn was discovered       https://githu b.com/Drizzl ingSun/Tend       0-TEN-AC18- 170523/2935	based Buffer	09-May-2023	2.7	been identified in SCALANCE LPE9403 (All versions < V2.1). A heap-based buffer overflow vulnerability was found in the `edgebox_web_app` binary. The binary will crash if supplied with a backup password longer than 255 characters. This could allow an authenticated privileged attacker to cause a denial of service. <b>CVE ID : CVE-2023-</b>	portal.sieme ns.com/prod uctcert/pdf/ ssa-			
Affected Version(s): 0.9         Improper Neutralizat ion of Special Elements used in an SQL ('SQL Injection')       04-May-2023       8.8       SQL injection vulnerability inSpryker Commerce OS 0.9 that allows for access to sensitive data via customer/order?ord erSearchForm[searc hText]= CVE ID : CVE-2023- 27568       N/A       0-SPR-COMM- 170523/2934         Vendor: Tenda         Vendor: Tenda         Tenda AC18 v15.03.05.19\(6318_) _cn was discovered       N/A         O'-SPR-COMM- 170523/2934         N/A         O-SPR-COMM- 170523/2934	Vendor: spr	yker						
Improper Neutralizat ion of Special Elements used in an SQL04-May-20238.8SQL inSpryker Commerce OS 0.9 that allows for access to sensitive data via customer/order?ord erSearchForm[searc hText]= CVE ID : CVE-2023- 27568N/A0-SPR-COMM- 170523/2934Vendor: Tendation (SQL Injection')04-May-20238.88.8Tenda AC18 v15.03.05.19\(6318\)_ cn was discoveredN/A0-SPR-COMM- 170523/2934Of May-20239.8Tenda AC18 v15.03.05.19(6318_) cn was discoveredN/A0-SPR-COMM- 170523/2934OF May-20239.8Tenda AC18 v15.03.05.19(6318_) cn was discoveredN/A0-TEN-AC18- 170523/2935	Product: co	mmerce_os						
Improper Neutralizat ion of Special Elements used in an SQL Command ('SQL Injection')04-May-20238.8vulnerability inSpryker Commerce OS 0.9 that allows for access to sensitive data via customer/order?ord erSearchForm[searc hText]= CVE ID : CVE-2023- 27568N/A0-SPR-COMM- 170523/2934Vendor: Tember Vendor: Tember Affected Version(s): 15.03.05.19\\(6318) ion ofN/A0-SPR-COMM- 170523/2934Improper Neutralizat ion of05-May-20239.8Tenda AC18 v15.03.05.19(6318_) _cn was discoveredhttps://githu b.com/Drizzl ingSun/Tend0-TEN-AC18- 170523/2935	Affected Ver	sion(s): 0.9						
Impection J       27568       Impection J	Neutralizat ion of Special Elements used in an SQL Command ('SQL	04-May-2023	8.8	vulnerability inSpryker Commerce OS 0.9 that allows for access to sensitive data via customer/order?ord erSearchForm[searc hText]=	N/A			
Product: ac18_firmware         Affected Version(s): 15.03.05.19\\(6318\)_cn         Improper       05-May-2023       9.8       Tenda AC18       https://githu       0-TEN-AC18-         Neutralizat       05-May-2023       9.8       Tenda AC18       b.com/Drizzl       1/0523/2935         .cn was discovered       ingSun/Tend       CVSS Scoring Scale       0-1       1-2       2-3       3-4       4-5       5-6       6-7       7-8       8-9       9-10	Injection')							
Affected Version(s): 15.03.05.19\\(6318\\)_cnImproper Neutralizat ion of05-May-20239.8Tenda AC18 v15.03.05.19(6318_) _cn was discoveredhttps://githu b.com/Drizzl ingSun/Tend0-TEN-AC18- 170523/2935CVSS Scoring Scale0-11-22-33-44-55-66-77-88-99-10	Vendor: Ter	nda			I	l		
Improper Neutralizat ion of05-May-20239.8Tenda AC18 v15.03.05.19(6318_) _cn was discoveredhttps://githu b.com/Drizzl ingSun/Tend0-TEN-AC18- 170523/2935CVSS Scoring Scale0-11-22-33-44-55-66-77-88-99-10	Product: ac18_firmware							
Neutralizat ion of       05-May-2023       9.8       v15.03.05.19(6318_)       b.com/Drizzl ingSun/Tend       0-TEN-AC18-170523/2935         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): 15.03.05	.19\\(631					
5	Neutralizat	05-May-2023	9.8	v15.03.05.19(6318_)	b.com/Drizzl			
Page <b>1101</b> of <b>1106</b>	CVSS Scoring S	Scale 0-1	1-2 2-3		6-7 7-8	8 8-9 9-10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Comman d Injection')			to contain a command injection vulnerability via the deviceName parameter in the setUsbUnload function.	a/blob/main /AC18/8/8. md	
			CVE ID : CVE-2023- 30135		
Product: n3	01_firmware				
Affected Ver	sion(s): 12.02.01	.61_multi			
Cleartext Transmissi on of Sensitive Informatio n	01-May-2023	5.7	Cleartext Transmission in cookie:ecos_pw: in Tenda N301 v6.0, firmware v12.03.01.06_pt allows an authenticated attacker on the LAN or WLAN to intercept communications with the router and obtain the password. <b>CVE ID : CVE-2023-</b>	N/A	0-TEN-N301- 170523/2936
Affected Ver	sion(s): 12 03 01	06 pt	29681		
Cleartext Transmissi on of Sensitive Informatio n	sion(s): 12.03.01 01-May-2023	5.7	Cleartext Transmission in set- cookie:ecos_pw: Tenda N301 v6.0, Firmware v12.02.01.61_multi allows an authenticated attacker on the LAN or WLAN to intercept communications with the router and obtain the password.	N/A	O-TEN-N301- 170523/2937

0-1

1-2

6-7 7-8

5-6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID : CVE-2023- 29680			
Vendor: tot	olink					
Product: a7	100ru_firmwar	e				
Affected Ver	sion(s): 7.4cu.23	13_b2019	1024			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	05-May-2023	9.8	TOTOLINK A7100RU V7.4cu.2313_B20191 024 is vulnerable to Command Injection. <b>CVE ID : CVE-2023-</b> <b>30053</b>	N/A	0-TOT-A710- 170523/2938	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	05-May-2023	9.8	TOTOLINK A7100RU V7.4cu.2313_B20191 024 has a Command Injection vulnerability. An attacker can obtain a stable root shell through a specially constructed payload. <b>CVE ID : CVE-2023-</b> <b>30054</b>	N/A	O-TOT-A710- 170523/2939	
Product: x5	000r_firmware					
Affected Ver	sion(s): 9.1.0u.61	18_b2020	)1102			
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	05-May-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B2020 1102 and V9.1.0u.6369_B2023 0113 contain a command insertion vulnerability in setting/setTracerout eCfg. This vulnerability allows an attacker to execute arbitrary	N/A	0-TOT-X500- 170523/2940	
CVSS Scoring Scale         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10           Page 1103 of 1106						

Page 1103 of 1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands through the "command" parameter.		
			CVE ID : CVE-2023- 30013		
Affected Ver	sion(s): 9.1.0u.63	69_b2023	0113	L	
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	05-May-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B2020 1102 and V9.1.0u.6369_B2023 0113 contain a command insertion vulnerability in setting/setTracerout eCfg. This vulnerability allows an attacker to execute arbitrary commands through the "command" parameter. <b>CVE ID : CVE-2023-</b> <b>30013</b>	N/A	0-TOT-X500- 170523/2941
Vendor: Zyx	kel				
-	g-418n_firmwa				
Affected Ver	sion(s): * Up to (i	ncluding)	1.00\\(aarp.13\\)c0		
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	01-May-2023	7.5	A cross-site scripting (XSS) vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote authenticated attacker with administrator privileges to store malicious scripts using a web management interface parameter,	https://ww w.zyxel.com /global/en/s upport/secu rity- advisories/z yxel- security- advisory-for- multiple- vulnerabiliti es-in-nbg- 418n-v2- home-router	O-ZYX-NBG 170523/2942

0-1

1-2

**2-3 3-4 4-5** Page **1104** of **1106**  5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in denial- of-service (DoS) conditions on an affected device.		
			CVE ID : CVE-2023- 22921		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-May-2023	7.5	A buffer overflow vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote unauthenticated attacker to cause DoS conditions by sending crafted packets if Telnet is enabled on a vulnerable device. <b>CVE ID : CVE-2023- 22922</b>	https://ww w.zyxel.com /global/en/s upport/secu rity- advisories/z yxel- security- advisory-for- multiple- vulnerabiliti es-in-nbg- 418n-v2- home-router	O-ZYX-NBG 170523/2943
Use of Externally- Controlled Format String	01-May-2023	6.5	A format string vulnerability in a binary of the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote authenticated attacker to cause denial-of-service (DoS) conditions on an affected device. <b>CVE ID : CVE-2023-</b> <b>22923</b>	https://ww w.zyxel.com /global/en/s upport/secu rity- advisories/z yxel- security- advisory-for- multiple- vulnerabiliti es-in-nbg- 418n-v2- home-router	0-ZYX-NBG 170523/2944
Buffer Copy without Checking Size of	01-May-2023	4.9	A buffer overflow vulnerability in the Zyxel NBG-418N v2 firmware versions prior to	https://ww w.zyxel.com /global/en/s upport/secu rity-	0-ZYX-NBG 170523/2945

0-1

1-2

2-33-44-5Page 1105 of 1106

5-6

6-7

7-8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID			
Input ('Classic Buffer Overflow')			V1.00(AARP.14)C0 could allow a remote authenticated attacker with administrator privileges to cause denial-of-service (DoS) conditions by executing crafted CLI commands on a vulnerable device.	advisories/z yxel- security- advisory-for- multiple- vulnerabiliti es-in-nbg- 418n-v2- home-router				
			CVE ID : CVE-2023- 22924					
Product: nbg6604_firmware								
Affected Version(s): 1.01\\(abir.0\\)c0								
Improper Neutralizat ion of Special Elements used in an OS Command ('OS Command Injection')	01-May-2023	8.8	The post- authentication command injection vulnerability in the Zyxel NBG6604 firmware version V1.01(ABIR.0)C0 could allow an authenticated attacker to execute some OS commands remotely by sending a crafted HTTP request. <b>CVE ID : CVE-2023- 22919</b>	https://ww w.zyxel.com /global/en/s upport/secu rity- advisories/z yxel- security- advisory-for- post- authenticatio n-command- injection- vulnerability -in-nbg6604- home-router	O-ZYX-NBG6- 170523/2946			

0-1

1-2

5-6