



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

16 - 31 Mar 2023

Vol. 10 No. 06

## Table of Content

Vendor	Product	Page Number
<b>Application</b>		
<b>accesspressthemes</b>	smart_logo_showcase_lite	1
	wp_popup_banners	10
<b>admin_log_project</b>	admin_log	18
<b>Adobe</b>	coldfusion	19
	creative_cloud	21
	dimension	22
	experience_manager	32
	experience_manager_cloud_service	40
	illustrator	48
<b>air_cargo_management_system_project</b>	air_cargo_management_system	52
<b>alphaware_-_simple_e-commerce_system_project</b>	alphaware_-_simple_e-commerce_system	53
<b>altanic</b>	no_api_amazon_affiliate	55
<b>amano</b>	xoffice	56
<b>ansible-semaphore</b>	ansible_semaphore	56
<b>answer</b>	answer	56
<b>Apache</b>	fineract	60
	inlong	61
	sling_resource_merger	62
	tomcat	63
<b>apiman</b>	apiman	65
<b>Arubanetworks</b>	clearpass_policy_manager	66
<b>askoc</b>	web_report_system	81
<b>automatic_question_paper_generator_system_project</b>	automatic_question_paper_generator_system	81

<b>Vendor</b>	<b>Product</b>	<b>Page Number</b>
<b>Aver</b>	ptzapp_2	85
<b>aveva</b>	aveva_plant_scada	85
	telemetry_server	86
<b>awsm</b>	embed_any_document	87
<b>Basercms</b>	basercms	87
<b>basixonline</b>	nex-forms	88
<b>booking-wp-plugin</b>	bookly	89
<b>Broadcom</b>	tcpreplay	89
<b>cal</b>	cal.com	91
<b>canteen_management_system_project</b>	canteen_management_system	92
<b>cerebrate-project</b>	cerebrate	93
<b>churchcrm</b>	churchcrm	94
<b>cilium</b>	cilium	94
	cilium-cli	101
<b>Cisco</b>	adaptive_security_appliance	103
	aironet_access_point_software	262
	catalyst_8000v_edge	262
	dna_center	263
	firepower_threat_defense	267
	wireless_lan_controller_software	426
<b>Ckeditor</b>	ckeditor	426
<b>cloudflare</b>	cloudflared	428
<b>Cminds</b>	cm_answers	430
<b>codemenschen</b>	gift_vouchers	430
<b>coder</b>	code-server	430
<b>collection.js_project</b>	collection.js	431
<b>corebos</b>	corebos	431
<b>couchbase</b>	couchbase_server	432
<b>courtbouillon</b>	cairosvg	432
<b>crmeb</b>	crmeb_java	433
<b>custom_content_shortcode_project</b>	custom_content_shortcode	434

Vendor	Product	Page Number
<b>databasir</b>	databasir	435
<b>dataease</b>	dataease	436
<b>datagear</b>	datagear	437
<b>Dedecms</b>	dedecms	439
<b>deltaww</b>	infrasuite_device_master	439
<b>deno</b>	deno	444
	deno_runtime	445
	serde_v8	446
<b>Dino</b>	dino	447
<b>discourse</b>	discourse	448
<b>dreamer_cms_project</b>	dreamer_cms	498
<b>e-commerce_system_project</b>	e-commerce_system	499
<b>e-dynamics</b>	events_made_easy	502
<b>earnings_and_expense_tracker_application_project</b>	earnings_and_expense_tracker_application	502
<b>earnings_and_expense_tracker_app_project</b>	earnings_and_expense_tracker_app	503
<b>ellucian</b>	banner_web_tailor	503
<b>evilmartians</b>	imgproxy	504
<b>evolucare</b>	ecs_imaging	505
<b>Extplorer</b>	extplorer	505
<b>Fedoraproject</b>	extra_packages_for_enterprise_linux	506
<b>feifeicms</b>	feifeicms	507
<b>file_management_system_project</b>	file_management_system	508
<b>Filseclab</b>	twister_antivirus	508
<b>fit2cloud</b>	jumpserver	510
	koko	511
<b>Flatpak</b>	Flatpak	511
<b>formidablepro2pdf</b>	formidable_pro2pdf	519

Vendor	Product	Page Number
<b>gadget_works_online_ordering_system_project</b>	gadget_works_online_ordering_system	520
<b>galaxyproject</b>	galaxy	520
<b>GE</b>	ifix	521
<b>generalbytes</b>	crypto_application_server	523
<b>Gentoo</b>	soko	523
<b>geosolutionsgroup</b>	geonode	524
<b>getresponse</b>	getresponse	529
<b>getshortcodes</b>	shortcodes_ultimate	530
<b>gmace_project</b>	gmace	531
<b>GNU</b>	org_mode	531
<b>go-huge-util_project</b>	go-huge-util	532
<b>Google</b>	chrome	532
	tensorflow	535
<b>gotowp</b>	gotowp	542
<b>gpac</b>	gpac	543
<b>grafana</b>	grafana	545
<b>greenshiftwp</b>	greenshift_-_animation_and_page_builder_blocks	547
<b>hasthemes</b>	contact_form_7_widget_for_elementor_page_builder_\&_gutenberg_blocks	548
	coupon_zen	548
	ever_compare	548
	free_woocommerce_theme_99fy_extension	549
	ht_event	549
	ht_politic	550
	ht_portfolio	550
	ht_slider_for_elementor	550
	preview_link_generator	551
	quickswish	551
	wc_sales_notification	551
	wp_education	552
	wp_film_studio	552

Vendor	Product	Page Number
<b>hasthemes</b>	wp_insurance	553
	wp_news	553
	wp_plugin_manager	553
<b>hgiga</b>	oakclouds_mailsherlock	554
	oakclouds_portal	555
<b>hkcms_project</b>	hkcms	556
<b>hu-manity</b>	cookie_notice_\&_compliance_for_gdpr_\/_ccp a	557
<b>IBM</b>	aspera_faspex	557
	security_key_lifecycle_manager	559
<b>ibos</b>	ibos	572
<b>Imagemagick</b>	imagemagick	573
<b>implecode</b>	ecommerce_product_catalog	574
<b>independentsoft</b>	jodf	575
	jspreadsheet	575
	jword	575
<b>invernyx</b>	smartcars_3	576
<b>Iobit</b>	malware_fighter	576
<b>isdecisions</b>	userlock	581
<b>jc21</b>	nginx_proxy_manager	582
<b>jeecg</b>	jeecg-boot	582
<b>Jenkins</b>	absint_a3	583
<b>jettison_project</b>	jettison	583
<b>Jiangmin</b>	jiangmin_antivirus	583
<b>joommasters</b>	jms_blog	586
<b>joomunited</b>	wp_meta_seo	586
<b>json-smart_project</b>	json-smart	587
<b>judging_management_system_project</b>	judging_management_system	588
<b>kaml_project</b>	kaml	588
<b>klaviyo</b>	klaviyo	589
<b>knplabs</b>	snappy	589
<b>ladybirdweb</b>	faveo_helpdesk	590

Vendor	Product	Page Number
<b>ladybirdweb</b>	faveo_servicedesk	591
<b>leadgenerated</b>	lead_generated	591
<b>lfprojects</b>	mlflow	592
<b>liblouis</b>	liblouis	593
<b>lightcms_project</b>	lightcms	594
<b>loan_management_system_project</b>	loan_management_system	594
<b>mage-people</b>	event_manager_and_tickets_selling_for_woocommerce	594
<b>mainwp</b>	code_snippets_extension	595
<b>Malwarebytes</b>	adwcleaner	595
	malwarebytes	595
<b>mattermost</b>	mattermost	596
<b>maxpcsecure</b>	anti_virus_plus	596
<b>Mcafee</b>	total_protection	599
<b>medical_certificate_generator_app_project</b>	medical_certificate_generator_app	599
<b>medicine_tracker_system_project</b>	medicine_tracker_system	600
<b>megamain</b>	mega_main_menu	602
<b>menu_shortcode_project</b>	menu_shortcode	602
<b>metagauss</b>	profilegrid	603
<b>mgt-commerce</b>	cloudpanel	603
<b>miniflux_project</b>	miniflux	604
<b>minio</b>	minio	606
<b>miniorange</b>	oauth_single_sign_on	608
<b>mirotalk</b>	mirotalk_p2p	609
<b>Misp-project</b>	malware_information_sharing_platform	609
<b>monitoring_of_students_cyber_accounts_system_project</b>	monitoring_of_students_cyber_accounts_system	610
<b>monospace</b>	directus	611
<b>Moodle</b>	moodle	612
<b>mp4v2_project</b>	mp4v2	625

Vendor	Product	Page Number
Netgate	Pfsense	626
	pfsense_plus	627
Nextcloud	nextcloud_server	627
Nextendweb	smart_slider_3	633
nooz_project	nooz	633
notrinos	notrinoserp	633
novel-plus_project	novel-plus	634
nsthemes	advanced_social_pixel	636
ofcms_project	ofcms	636
omicronenergy	stationguard	636
	stationscout	637
onekeyadmin	onekeyadmin	638
online_book_store_project	online_book_store_project	638
online_exam_software_\	_eexamhall_project	639
online_food_ordering_system_project	online_food_ordering_system	639
online_pizza_ordering_system_project	online_pizza_ordering_system	640
online_tours_\&_travels_management_system_project	online_tours_\&_travels_management_system	641
oohboi_steroids_for_elementor_project	oohboi_steroids_for_elementor	642
oopspam	oopspam_anti-spam	643
Openbsd	openssh	643
openfind	mail2000	643
opengoofy	hippo4j	644
Opennms	horizon	645
	meridian	646
Openssl	openssl	649
otcms	otcms	652
Otrs	otrs	653
pacrapor	pacrapor	656

Vendor	Product	Page Number
<b>page_loading_effects_project</b>	page_loading_effects	656
<b>parity</b>	frontier	657
<b>park_ticketing_management_system_project</b>	park_ticketing_management_system	658
<b>pdfio_project</b>	pdfio	658
<b>Pfsense</b>	pfsense	659
<b>Pimcore</b>	pimcore	659
<b>pixedelic</b>	camera_slideshow	663
<b>play-with-docker</b>	play_with_docker	664
<b>Pluck-cms</b>	pluck	665
<b>plugin</b>	waiting	667
<b>pluginus</b>	inpost_gallery	668
	wordpress_meta_data_and_taxonomies_filter	668
<b>Postgresql</b>	pgadmin_4	669
<b>Prestashop</b>	eo_tags	669
<b>Qemu</b>	qemu	670
<b>Qibosoft</b>	qibocms	670
<b>qykcms</b>	qykcms	670
<b>Radare</b>	radare2	671
<b>Rapid7</b>	insightappsec	672
	insightcloudsec	673
	insightvm	675
<b>rapidload</b>	rapidload_power-up_for_autooptimize	675
<b>react_webcam_project</b>	react_webcam	676
<b>real.kit_project</b>	real.kit	676
<b>really-simple-plugins</b>	complianz	677
<b>redis</b>	redis	677
<b>request_project</b>	request	678
<b>responsive_hotel_site_project</b>	responsive_hotel_site	678
<b>rifartek</b>	iot_wall	679
<b>rockoa</b>	rockoa	680

Vendor	Product	Page Number
<b>Rockwellautomation</b>	modbus_tcp_server_add_on_instructions	680
	thinmanager	681
<b>ruifang-tech</b>	rebuild	692
<b>russh_project</b>	russh	695
<b>saan</b>	world_clock	697
<b>saml_project</b>	saml	697
<b>Samsung</b>	bixbytouch	698
	calendar	698
	myfiles	699
	quick_share	700
<b>schedulicity</b>	schedulicity	701
<b>Schneider-electric</b>	custom_reports	701
	igss_dashboard	707
	igss_data_server	712
<b>school_registration_and_fee_system_project</b>	school_registration_and_fee_system	717
<b>sentry</b>	sentry_software_development_kit	717
<b>service_area_postcode_checker_project</b>	service_area_postcode_checker	719
<b>silabs</b>	wi-sun_software_development_kit	719
<b>Silverstripe</b>	graphql	720
<b>simplefilelist</b>	simple_file_list	721
<b>simple_and_beautiful_shopping_cart_system_project</b>	simple_and_beautiful_shopping_cart_system	722
<b>simple_and_nice_shopping_cart_script_project</b>	simple_and_nice_shopping_cart_script	722
<b>simple_art_gallery_project</b>	simple_art_gallery	723
<b>simple_customer_relationship_management_system_project</b>	simple_customer_relationship_management_system	724
<b>simple_image_gallery_web_app_project</b>	simple_image_gallery_web_app	724

Vendor	Product	Page Number
<b>simple_music_player_project</b>	simple_music_player	725
<b>simple_online_hotel_reservation_system_project</b>	simple_online_hotel_reservation_system	725
<b>simplygallery</b>	simply_gallery_blocks_with_lightbox	726
<b>smpredirectionsmanager_project</b>	smpredirectionsmanager	727
<b>softmaker</b>	flexipdf	727
<b>squidex.io</b>	squidex	727
<b>storage_unit_rental_management_system_project</b>	storage_unit_rental_management_system	728
<b>strangerstudios</b>	paid_memberships_pro	728
<b>strategy11</b>	formidable_form_builder	729
<b>streamlit</b>	streamlit	729
<b>student_study_center_desk_management_system_project</b>	student_study_center_desk_management_system	730
<b>sudo_project</b>	sudo	734
<b>superior_faq_project</b>	superior_faq	734
<b>Swftools</b>	swftools	735
<b>tailscale</b>	tailscale	735
<b>task_allocation_system_project</b>	task_allocation_system	736
<b>teachpress_project</b>	teachpress	737
<b>teacms_project</b>	teacms	737
<b>Teampass</b>	teampass	738
<b>technocrackers</b>	bulk_price_update_for_woocommerce	739
<b>temenos</b>	t24	740
<b>templatesnext</b>	templatesnext_toolkit	740
<b>tinydng_project</b>	tinydng	740
<b>tinytiff_project</b>	tinytiff	741
<b>Tipsandtricks-hq</b>	wordpress_simple_paypal_shopping_cart	742
	wp_express_checkout	743

Vendor	Product	Page Number
<b>top_10_-_popular_posts_project</b>	top_10_-_popular_posts	743
<b>tosec</b>	kirin_fortress_machine	744
<b>Trendmicro</b>	trend_micro_endpoint_encryption	744
	txone_stellarone	745
<b>tribe29</b>	checkmk	746
<b>trudesk_project</b>	trudesk	747
<b>tshirtecommerce</b>	tshirtecommerce	747
<b>typecho</b>	typecho	748
<b>university_information_management_system_project</b>	university_information_management_system	749
<b>utarit</b>	persolus	749
<b>vadi</b>	digikent	750
<b>vektor-inc</b>	vk_all_in_one_expansion_unit	750
<b>Veritas</b>	aptare_it_analytics	751
	netbackup	751
	netbackup_it_analytics	752
<b>veronalabs</b>	wp_statistics	753
<b>versionize_project</b>	versionize	754
<b>very_simple_google_maps_project</b>	very_simple_google_maps	755
<b>Vmware</b>	spring_cloud_config	755
	spring_cloud_vault	756
	spring_framework	756
	spring_vault	758
<b>vox2mesh_project</b>	vox2mesh	758
<b>vxsearch</b>	vx_search	759
<b>watchdog</b>	anti-virus	760
<b>water_billing_system_project</b>	water_billing_system	761
<b>webnus</b>	modern_events_calendar_lite	761
<b>westerndigital</b>	sandisk_privateaccess	762
<b>winwar</b>	wp_etsy_product_feeds	762

Vendor	Product	Page Number
winwar	wp_flipclock	762
wisdomgarden	tronclass_ilearn	763
wisecleaner	wise_force_deleter	764
	wise_system_monitor	764
woocommerce_multiple_customer_addresses_&_shipping_project	woocommerce_multiple_customer_addresses_&_shipping	766
wp-commentnavi_project	wp-commentnavi	767
wp-master	feed_changer_&_remover	767
wp-slimstat	slimstat_analytics	768
wpbean	wpb_advanced_faq	768
wpmobile.app_project	wpmobile.app	769
wppool	wp_dark_mode	769
wpvar	wp_shamsi	769
wp_better_emails_project	wp_better_emails	770
wp_htpasswd_project	wp_htpasswd	770
wp_image_carousel_project	wp_image_carousel	770
wp_popup_banners_project	wp_popup_banners	771
X.org	x_server	771
xipblog_project	xipblog	772
xpdfreader	xpdf	772
xuxueli	xxl-job	773
xzjie_cms_project	xzjie_cms	774
young_entrepreneur_e-negosyo_system_project	young_entrepreneur_e-negosyo_system	774
Zoom	meetings	776
	rooms	776
	virtual_desktop_infrastructure	777
	zoom	778
<b>Hardware</b>		

Vendor	Product	Page Number
<b>360</b>	d901	779
<b>centralite</b>	pearl	780
<b>Cisco</b>	8101-32fh	780
	8101-32h	782
	8102-64h	785
	8201	787
	8201-32fh	789
	8202	791
	8800_12-slot	794
	8800_18-slot	796
	8800_4-slot	798
	8800_8-slot	800
	8804	803
	8808	805
	8812	807
	8818	809
	8831	812
	9800-40	814
	9800-80	815
	9800-cl	817
	9800-l	818
	aironet_1540	819
	aironet_1542d	820
	aironet_1542i	821
	aironet_1560	821
	aironet_1562d	822
	aironet_1562e	823
	aironet_1562i	823
	aironet_1800	824
	aironet_1800i	825
	aironet_1810	825
	aironet_1810w	826

Vendor	Product	Page Number
<b>Cisco</b>	aironet_1815	827
	aironet_1815i	827
	aironet_1815m	828
	aironet_1815t	829
	aironet_1815w	829
	aironet_2800	830
	aironet_2800e	831
	aironet_2800i	831
	aironet_3800	832
	aironet_3800e	833
	aironet_3800i	833
	aironet_3800p	834
	aironet_4800	835
	asr_1000	835
	asr_1000-esp100	838
	asr_1000-esp100-x	840
	asr_1000-esp200-x	842
	asr_1000-x	844
	asr_1001	845
	asr_1001-hx	848
	asr_1001-hx_r	850
	asr_1001-x	851
	asr_1001-x_r	854
	asr_1002	857
	asr_1002-hx	859
	asr_1002-hx_r	862
	asr_1002-x	864
	asr_1002-x_r	867
	asr_1004	869
	asr_1006	871
	asr_1006-x	873
asr_1009-x	876	

Vendor	Product	Page Number
<b>Cisco</b>	asr_1013	880
	asr_1023	882
	asr_900	884
	asr_9000	886
	asr_9000v	889
	asr_9001	893
	asr_9006	895
	asr_901-12c-f-d	897
	asr_901-12c-ft-d	899
	asr_901-4c-f-d	900
	asr_901-4c-ft-d	902
	asr_901-6cz-f-a	903
	asr_901-6cz-f-d	904
	asr_901-6cz-fs-a	906
	asr_901-6cz-fs-d	907
	asr_901-6cz-ft-a	908
	asr_901-6cz-ft-d	910
	asr_9010	911
	asr_901s-2sg-f-ah	913
	asr_901s-2sg-f-d	915
	asr_901s-3sg-f-ah	916
	asr_901s-3sg-f-d	917
	asr_901s-4sg-f-d	919
	asr_902	920
	asr_902u	922
	asr_903	925
	asr_907	927
	asr_914	929
	asr_920-10sz-pd	931
	asr_920-10sz-pd_r	932
	asr_920-12cz-a	933
asr_920-12cz-a_r	935	

Vendor	Product	Page Number
Cisco	asr_920-12cz-d	936
	asr_920-12cz-d_r	937
	asr_920-12sz-im	939
	asr_920-12sz-im_r	940
	asr_920-24sz-im	942
	asr_920-24sz-im_r	943
	asr_920-24sz-m	944
	asr_920-24sz-m_r	946
	asr_920-24tz-m	947
	asr_920-24tz-m_r	948
	asr_920-4sz-a	950
	asr_920-4sz-a_r	951
	asr_920-4sz-d	952
	asr_920-4sz-d_r	954
	asr_920u-12sz-im	955
	asr_9901	957
	asr_9902	958
	asr_9903	959
	asr_9904	961
	asr_9906	962
	asr_9910	963
	asr_9912	965
	asr_9920	966
	asr_9922	968
	catalyst_3650	969
	catalyst_3650-12x48fd-e	970
	catalyst_3650-12x48fd-l	971
	catalyst_3650-12x48fd-s	972
	catalyst_3650-12x48uq	973
	catalyst_3650-12x48uq-e	974
	catalyst_3650-12x48uq-l	975
	catalyst_3650-12x48uq-s	975

Vendor	Product	Page Number
<b>Cisco</b>	catalyst_3650-12x48ur	977
	catalyst_3650-12x48ur-e	977
	catalyst_3650-12x48ur-l	978
	catalyst_3650-12x48ur-s	979
	catalyst_3650-12x48uz	981
	catalyst_3650-12x48uz-e	981
	catalyst_3650-12x48uz-l	982
	catalyst_3650-12x48uz-s	983
	catalyst_3650-24pd	985
	catalyst_3650-24pd-e	985
	catalyst_3650-24pd-l	986
	catalyst_3650-24pd-s	987
	catalyst_3650-24pdm	989
	catalyst_3650-24pdm-e	989
	catalyst_3650-24pdm-l	990
	catalyst_3650-24pdm-s	991
	catalyst_3650-24ps-e	992
	catalyst_3650-24ps-l	993
	catalyst_3650-24ps-s	994
	catalyst_3650-24td-e	995
	catalyst_3650-24td-l	996
	catalyst_3650-24td-s	997
	catalyst_3650-24ts-e	998
	catalyst_3650-24ts-l	999
	catalyst_3650-24ts-s	1000
	catalyst_3650-48fd-e	1001
	catalyst_3650-48fd-l	1002
	catalyst_3650-48fd-s	1003
	catalyst_3650-48fq	1005
	catalyst_3650-48fq-e	1005
catalyst_3650-48fq-l	1006	
catalyst_3650-48fq-s	1007	

Vendor	Product	Page Number
<b>Cisco</b>	catalyst_3650-48fqm	1009
	catalyst_3650-48fqm-e	1009
	catalyst_3650-48fqm-l	1010
	catalyst_3650-48fqm-s	1011
	catalyst_3650-48fs-e	1012
	catalyst_3650-48fs-l	1013
	catalyst_3650-48fs-s	1014
	catalyst_3650-48pd-e	1015
	catalyst_3650-48pd-l	1016
	catalyst_3650-48pd-s	1017
	catalyst_3650-48pq-e	1018
	catalyst_3650-48pq-l	1019
	catalyst_3650-48pq-s	1020
	catalyst_3650-48ps-e	1021
	catalyst_3650-48ps-l	1022
	catalyst_3650-48ps-s	1023
	catalyst_3650-48td-e	1024
	catalyst_3650-48td-l	1025
	catalyst_3650-48td-s	1026
	catalyst_3650-48tq-e	1027
	catalyst_3650-48tq-l	1028
	catalyst_3650-48tq-s	1029
	catalyst_3650-48ts-e	1030
	catalyst_3650-48ts-l	1031
	catalyst_3650-48ts-s	1032
	catalyst_3650-8x24pd-e	1033
	catalyst_3650-8x24pd-l	1034
	catalyst_3650-8x24pd-s	1035
	catalyst_3650-8x24uq	1037
	catalyst_3650-8x24uq-e	1037
	catalyst_3650-8x24uq-l	1038
catalyst_3650-8x24uq-s	1039	

Vendor	Product	Page Number
<b>Cisco</b>	catalyst_3850	1040
	catalyst_3850-12s-e	1043
	catalyst_3850-12s-s	1045
	catalyst_3850-12x48u	1047
	catalyst_3850-12xs-e	1049
	catalyst_3850-12xs-s	1052
	catalyst_3850-16xs-e	1054
	catalyst_3850-16xs-s	1056
	catalyst_3850-24p-e	1058
	catalyst_3850-24p-l	1061
	catalyst_3850-24p-s	1063
	catalyst_3850-24pw-s	1065
	catalyst_3850-24s-e	1067
	catalyst_3850-24s-s	1070
	catalyst_3850-24t-e	1072
	catalyst_3850-24t-l	1074
	catalyst_3850-24t-s	1076
	catalyst_3850-24u	1079
	catalyst_3850-24u-e	1081
	catalyst_3850-24u-l	1083
	catalyst_3850-24u-s	1085
	catalyst_3850-24xs	1088
	catalyst_3850-24xs-e	1090
	catalyst_3850-24xs-s	1092
	catalyst_3850-24xu	1094
	catalyst_3850-24xu-e	1097
	catalyst_3850-24xu-l	1099
	catalyst_3850-24xu-s	1101
	catalyst_3850-32xs-e	1103
	catalyst_3850-32xs-s	1106
catalyst_3850-48f-e	1108	
catalyst_3850-48f-l	1110	

Vendor	Product	Page Number
<b>Cisco</b>	catalyst_3850-48f-s	1112
	catalyst_3850-48p-e	1115
	catalyst_3850-48p-l	1117
	catalyst_3850-48p-s	1119
	catalyst_3850-48pw-s	1121
	catalyst_3850-48t-e	1124
	catalyst_3850-48t-l	1126
	catalyst_3850-48t-s	1128
	catalyst_3850-48u	1130
	catalyst_3850-48u-e	1133
	catalyst_3850-48u-l	1135
	catalyst_3850-48u-s	1137
	catalyst_3850-48xs	1139
	catalyst_3850-48xs-e	1142
	catalyst_3850-48xs-f-e	1144
	catalyst_3850-48xs-f-s	1146
	catalyst_3850-48xs-s	1148
	catalyst_3850-nm-2-40g	1151
	catalyst_3850-nm-8-10g	1153
	catalyst_8200	1155
	catalyst_8300	1158
	catalyst_8300-1n1s-4t2x	1161
	catalyst_8300-1n1s-6t	1164
	catalyst_8300-2n2s-4t2x	1167
	catalyst_8300-2n2s-6t	1170
	catalyst_8500	1173
	catalyst_8500-4qc	1175
	catalyst_8500l	1178
	catalyst_8510csr	1182
	catalyst_8510msr	1185
catalyst_8540csr	1188	
catalyst_8540msr	1191	

Vendor	Product	Page Number
<b>Cisco</b>	catalyst_9100	1194
	catalyst_9105	1195
	catalyst_9105ax	1195
	catalyst_9105axi	1196
	catalyst_9105axw	1197
	catalyst_9115	1197
	catalyst_9115ax	1198
	catalyst_9115axe	1199
	catalyst_9115axi	1199
	catalyst_9115_ap	1200
	catalyst_9117	1201
	catalyst_9117ax	1201
	catalyst_9117axi	1202
	catalyst_9117_ap	1203
	catalyst_9120	1203
	catalyst_9120ax	1204
	catalyst_9120axe	1205
	catalyst_9120axi	1205
	catalyst_9120axp	1206
	catalyst_9120_ap	1207
	catalyst_9124	1207
	catalyst_9124ax	1208
	catalyst_9124axd	1209
	catalyst_9124axi	1209
	catalyst_9130	1210
	catalyst_9130ax	1211
	catalyst_9130axe	1211
	catalyst_9130axi	1212
	catalyst_9130_ap	1213
	catalyst_9200	1213
	catalyst_9200cx	1216
catalyst_9200l	1218	

Vendor	Product	Page Number
<b>Cisco</b>	catalyst_9300	1220
	catalyst_9300-24p-a	1223
	catalyst_9300-24p-e	1227
	catalyst_9300-24s-a	1230
	catalyst_9300-24s-e	1233
	catalyst_9300-24t-a	1237
	catalyst_9300-24t-e	1240
	catalyst_9300-24u-a	1243
	catalyst_9300-24u-e	1247
	catalyst_9300-24ux-a	1250
	catalyst_9300-24ux-e	1253
	catalyst_9300-48p-a	1257
	catalyst_9300-48p-e	1260
	catalyst_9300-48s-a	1263
	catalyst_9300-48s-e	1266
	catalyst_9300-48t-a	1270
	catalyst_9300-48t-e	1273
	catalyst_9300-48u-a	1276
	catalyst_9300-48u-e	1280
	catalyst_9300-48un-a	1283
	catalyst_9300-48un-e	1286
	catalyst_9300-48uxm-a	1290
	catalyst_9300-48uxm-e	1293
	catalyst_9300l	1296
	catalyst_9300l-24p-4g-a	1299
	catalyst_9300l-24p-4g-e	1303
	catalyst_9300l-24p-4x-a	1306
	catalyst_9300l-24p-4x-e	1309
	catalyst_9300l-24t-4g-a	1313
	catalyst_9300l-24t-4g-e	1316
	catalyst_9300l-24t-4x-a	1319
	catalyst_9300l-24t-4x-e	1323

Vendor	Product	Page Number
Cisco	catalyst_9300l-48p-4g-a	1326
	catalyst_9300l-48p-4g-e	1329
	catalyst_9300l-48p-4x-a	1332
	catalyst_9300l-48p-4x-e	1336
	catalyst_9300l-48t-4g-a	1339
	catalyst_9300l-48t-4g-e	1342
	catalyst_9300l-48t-4x-a	1346
	catalyst_9300l-48t-4x-e	1349
	catalyst_9300lm	1352
	catalyst_9300l_stack	1356
	catalyst_9300x	1359
	catalyst_9400	1362
	catalyst_9400_supervisor_engine-1	1364
	catalyst_9407r	1367
	catalyst_9410r	1369
	catalyst_9500	1371
	catalyst_9500h	1373
	catalyst_9600	1376
	catalyst_9600x	1378
	catalyst_9600_supervisor_engine-1	1380
	catalyst_9800	1382
	catalyst_9800-40	1385
	catalyst_9800-40_wireless_controller	1387
	catalyst_9800-80	1389
	catalyst_9800-80_wireless_controller	1391
	catalyst_9800-cl	1394
	catalyst_9800-l	1396
	catalyst_9800-l-c	1398
	catalyst_9800-l-f	1400
	catalyst_9800_embedded_wireless_controller	1403
	catalyst_ie3200	1405
	catalyst_ie3200_rugged_switch	1406

Vendor	Product	Page Number
Cisco	catalyst_ie3300	1408
	catalyst_ie3300_rugged_switch	1409
	catalyst_ie3400	1410
	catalyst_ie3400_heavy_duty_switch	1412
	catalyst_ie3400_rugged_switch	1413
	catalyst_ie9300	1414
	catalyst_iw6300	1416
	catalyst_iw6300_ac	1416
	catalyst_iw6300_dc	1417
	catalyst_iw6300_dcw	1418
	cbr-8	1418
	cbr8_converged_broadband_router	1420
	cg418-e	1421
	cg522-e	1423
	cloud_services_router_1000v	1425
	csr_1000v	1426
	esr-6300-con-k9	1427
	esr-6300-ncp-k9	1428
	esr6300	1429
	ess-3300-24t-con-a	1430
	ess-3300-24t-con-e	1433
	ess-3300-24t-ncp-a	1435
	ess-3300-24t-ncp-e	1437
	ess-3300-con-a	1439
	ess-3300-con-e	1442
	ess-3300-ncp-a	1444
	ess-3300-ncp-e	1446
	ess9300-10x-e	1448
	esw6300	1451
	ie-3200-8p2s-e	1451
	ie-3200-8t2s-e	1452
	ie-3300-8p2s-a	1453

Vendor	Product	Page Number
Cisco	ie-3300-8p2s-e	1454
	ie-3300-8t2s-a	1455
	ie-3300-8t2s-e	1456
	ie-3300-8t2x-a	1457
	ie-3300-8t2x-e	1458
	ie-3300-8u2x-a	1459
	ie-3300-8u2x-e	1460
	ie-3400-8p2s-a	1461
	ie-3400-8p2s-e	1462
	ie-3400-8t2s-a	1463
	ie-3400-8t2s-e	1464
	ie-9310-26s2c	1464
	ie-9320-26s2c	1465
	integrated_services_virtual_router	1466
	isr_1000	1469
	isr_1100	1470
	isr_1100-4g	1472
	isr_1100-4g\6g	1475
	isr_1100-4p	1475
	isr_1100-6g	1479
	isr_1100-8p	1481
	isr_1101	1484
	isr_1101-4p	1487
	isr_1109	1490
	isr_1109-2p	1493
	isr_1109-4p	1497
	isr_1111x	1500
	isr_1111x-8p	1502
	isr_111x	1504
	isr_1120	1506
	isr_1131	1510
	isr_1160	1513

Vendor	Product	Page Number
<b>Cisco</b>	isr_4000	1516
	isr_4221	1518
	isr_4321	1521
	isr_4331	1524
	isr_4351	1527
	isr_4431	1531
	isr_4451	1534
	isr_4451-x	1537
	isr_4461	1540
<b>dek-1705_project</b>	dek-1705	1543
<b>Dell</b>	embedded_box_pc_3000	1543
<b>Dlink</b>	dir820la1	1544
<b>hgiga</b>	powerstation	1544
<b>hpe</b>	apollo_4200_gen10_plus_system	1545
	apollo_4200_gen10_server	1546
	apollo_4200_gen9_server	1546
	apollo_4510_gen10_system	1546
	apollo_6500_gen10_plus_system	1547
	apollo_6500_gen10_system	1547
	apollo_n2600_gen10_plus	1548
	apollo_n2800_gen10_plus	1548
	apollo_r2000_chassis	1548
	apollo_r2200_gen10	1549
	apollo_r2600_gen10	1549
	apollo_r2800_gen10	1550
	aruba_cx_10000-48y6	1550
	aruba_cx_6200f_48g	1550
	aruba_cx_6200m_24g	1551
	aruba_cx_6300m_24p	1551
	aruba_cx_6300m_48g	1552
	aruba_cx_6405	1552
aruba_cx_6410	1553	

Vendor	Product	Page Number
hpe	aruba_cx_8320-32	1553
	aruba_cx_8320-48p	1554
	aruba_cx_8325-32c	1554
	aruba_cx_8325-48y8c	1554
	aruba_cx_8360-12c	1555
	aruba_cx_8360-16y2c	1555
	aruba_cx_8360-24xf2c	1556
	aruba_cx_8360-32y4c	1556
	aruba_cx_8360-48xt4c	1557
	aruba_cx_8360-48y6c	1557
	aruba_cx_8400	1558
	aruba_cx_9300_32d	1558
	edgeline_e920d_server_blade	1558
	edgeline_e920t_server_blade	1559
	edgeline_e920_server_blade	1559
	proliant_bl420c_gen8_server	1560
	proliant_bl460c_gen10_server_blade	1560
	proliant_bl460c_gen8_server_blade	1560
	proliant_bl460c_gen9_server_blade	1561
	proliant_bl465c_gen8_server_blade	1561
	proliant_bl660c_gen8_server_blade	1562
	proliant_bl660c_gen9_server	1562
	proliant_dl120_gen10_server	1562
	proliant_dl120_gen9_server	1563
	proliant_dl160_gen10_server	1563
	proliant_dl160_gen8_server	1564
	proliant_dl160_gen9_server	1564
	proliant_dl180_gen10_server	1564
	proliant_dl180_gen9_server	1565
	proliant_dl20_gen10_plus_server	1565
	proliant_dl20_gen10_server	1566
	proliant_dl20_gen9_server	1566

Vendor	Product	Page Number
hpe	proliant_dl320e_gen8_server	1566
	proliant_dl320e_gen8_v2_server	1567
	proliant_dl320_gen11_server	1567
	proliant_dl325_gen10_plus_server	1568
	proliant_dl325_gen10_server	1568
	proliant_dl325_gen11_server	1568
	proliant_dl345_gen10_plus_server	1569
	proliant_dl345_gen11_server	1569
	proliant_dl360e_gen8_server	1570
	proliant_dl360p_gen8_server	1570
	proliant_dl360_gen10_plus_server	1570
	proliant_dl360_gen10_server	1571
	proliant_dl360_gen11_server	1571
	proliant_dl360_gen9_server	1572
	proliant_dl365_gen10_plus_server	1572
	proliant_dl365_gen11_server	1572
	proliant_dl380e_gen8_server	1573
	proliant_dl380p_gen8_server	1573
	proliant_dl380_gen10_plus_server	1574
	proliant_dl380_gen10_server	1574
	proliant_dl380_gen11_server	1574
	proliant_dl380_gen9_server	1575
	proliant_dl385p_gen8_(amd\)	1575
	proliant_dl385_gen10_plus_server	1576
	proliant_dl385_gen10_plus_v2_server	1576
	proliant_dl385_gen10_server	1576
	proliant_dl385_gen11_server	1577
	proliant_dl560_gen10_server	1577
	proliant_dl560_gen8_server	1578
	proliant_dl560_gen9_server	1578
	proliant_dl580_gen10_server	1578
	proliant_dl580_gen8_server	1579

Vendor	Product	Page Number
hpe	proliant_dl580_gen9_server	1579
	proliant_dl60_gen9_server	1580
	proliant_dl80_gen9_server	1580
	proliant_dx170r_gen10_server	1580
	proliant_dx190r_gen10_server	1581
	proliant_dx220n_gen10_plus_server	1581
	proliant_dx325_gen10_plus_v2_server	1582
	proliant_dx360_gen10_plus_server	1582
	proliant_dx360_gen10_server	1582
	proliant_dx380_gen10_plus_server	1583
	proliant_dx380_gen10_server	1583
	proliant_dx385_gen10_plus_server	1584
	proliant_dx385_gen10_plus_v2_server	1584
	proliant_dx4200_gen10_server	1584
	proliant_dx560_gen10_server	1585
	proliant_e910t_server_blade	1585
	proliant_e910_server_blade	1586
	proliant_microserver_gen8	1586
	proliant_ml110_gen10_server	1586
	proliant_ml110_gen9_server	1587
	proliant_ml30_gen10_plus_server	1587
	proliant_ml30_gen9_server	1588
	proliant_ml310e_gen8_server	1588
	proliant_ml310e_gen8_v2_server	1588
	proliant_ml350e_gen8_server	1589
	proliant_ml350e_gen8_v2_server	1589
	proliant_ml350p_gen8_server	1590
	proliant_ml350_gen10_server	1590
	proliant_ml350_gen11_server	1590
	proliant_ml350_gen9_server	1591
	proliant_sl210t_gen8_server	1591
	proliant_sl230s_gen8_server	1592

Vendor	Product	Page Number
hpe	proliant_sl250s_gen8_server	1592
	proliant_sl270s_gen8_server	1592
	proliant_sl270s_gen8_se_server	1593
	proliant_ws460c_gen8_graphics_server_blade	1593
	proliant_ws460c_gen9_graphics_server_blade	1594
	proliant_xl170r_gen10_server	1594
	proliant_xl170r_gen9_server	1594
	proliant_xl190r_gen10_server	1595
	proliant_xl190r_gen9_server	1595
	proliant_xl220a_gen8_v2_server	1596
	proliant_xl220n_gen10_plus_server	1596
	proliant_xl225n_gen10_plus_1u_node	1596
	proliant_xl230a_gen9_server	1597
	proliant_xl230b_gen9_server	1597
	proliant_xl230k_gen10_server	1598
	proliant_xl250a_gen9_server	1598
	proliant_xl270d_gen10_server	1598
	proliant_xl270d_gen9_special_server	1599
	proliant_xl290n_gen10_plus_server	1599
	proliant_xl450_gen10_server	1600
	proliant_xl450_gen9_server	1600
	proliant_xl645d_gen10_plus_server	1600
	proliant_xl675d_gen10_plus_server	1601
	proliant_xl730f_gen9_server	1601
	proliant_xl740f_gen9_server	1602
	proliant_xl750f_gen9_server	1602
	storage_file_controller	1602
	storage_performance_file_controller	1603
	storeeasy_1430_storage	1603
	storeeasy_1440_storage	1604
	storeeasy_1450_storage	1604
	storeeasy_1460_storage	1604

Vendor	Product	Page Number
hpe	storeeasy_1530_storage	1605
	storeeasy_1540_storage	1605
	storeeasy_1550_storage	1606
	storeeasy_1560_storage	1606
	storeeasy_1630_storage	1606
	storeeasy_1640_storage	1607
	storeeasy_1650_expanded_storage	1607
	storeeasy_1650_storage	1608
	storeeasy_1660_expanded_storage	1608
	storeeasy_1660_performance_storage	1608
	storeeasy_1660_storage	1609
	storeeasy_1830_storage	1609
	storeeasy_1840_storage	1610
	storeeasy_1850_storage	1610
	storeeasy_1860_performance_storage	1610
	storeeasy_1860_storage	1611
	storeeasy_3830_gateway_storage	1611
	storeeasy_3830_gateway_storage_blade	1612
	storeeasy_3840_gateway_storage	1612
	storeeasy_3840_gateway_storage_blade	1612
	storeeasy_3850_gateway_single_node_upgrade	1613
	storeeasy_3850_gateway_storage	1613
	storeeasy_3850_gateway_storage_blade	1614
	storevirtual_3000_file_controller	1614
	synergy_480_gen10_compute_module	1614
	synergy_480_gen10_plus_compute_module	1615
	synergy_480_gen9_compute_module	1615
	synergy_620_gen9_compute_module	1616
	synergy_660_gen10_compute_module	1616
	synergy_660_gen9_compute_module	1616
synergy_680_gen9_compute_module	1617	
jcgcn.com	jhr-n916r	1617

Vendor	Product	Page Number
<b>Iancombg</b>	sa-wr915nd	1618
<b>Omron</b>	sysmac_cj2h-cpu64	1618
	sysmac_cj2h-cpu64-eip	1618
	sysmac_cj2h-cpu65	1619
	sysmac_cj2h-cpu65-eip	1619
	sysmac_cj2h-cpu66	1620
	sysmac_cj2h-cpu66-eip	1621
	sysmac_cj2h-cpu67	1621
	sysmac_cj2h-cpu67-eip	1622
	sysmac_cj2h-cpu68	1622
	sysmac_cj2h-cpu68-eip	1623
	sysmac_cj2m-cpu11	1623
	sysmac_cj2m-cpu12	1624
	sysmac_cj2m-cpu13	1624
	sysmac_cj2m-cpu14	1625
	sysmac_cj2m-cpu15	1626
	sysmac_cj2m-cpu31	1626
	sysmac_cj2m-cpu32	1627
	sysmac_cj2m-cpu33	1627
	sysmac_cj2m-cpu34	1628
	sysmac_cj2m-cpu35	1628
	sysmac_cp1e-e10dr-a	1629
	sysmac_cp1e-e10dr-d	1629
	sysmac_cp1e-e10dt-a	1630
	sysmac_cp1e-e10dt-d	1631
	sysmac_cp1e-e10dt1-a	1631
	sysmac_cp1e-e10dt1-d	1632
	sysmac_cp1e-e14dr-a	1632
	sysmac_cp1e-e14sdr-a	1633
	sysmac_cp1e-e20dr-a	1633
	sysmac_cp1e-e20sdr-a	1634
	sysmac_cp1e-e30dr-a	1634

Vendor	Product	Page Number
<b>Omron</b>	sysmac_cp1e-e30sdr-a	1635
	sysmac_cp1e-e40dr-a	1636
	sysmac_cp1e-e40sdr-a	1636
	sysmac_cp1e-e60sdr-a	1637
	sysmac_cp1e-na20dr-a	1637
	sysmac_cp1e-na20dt-d	1638
	sysmac_cp1e-na20dt1-d	1638
	sysmac_cp1h-x40dr-a	1639
	sysmac_cp1h-x40dt-d	1639
	sysmac_cp1h-x40dt1-d	1640
	sysmac_cp1h-xa40dr-a	1641
	sysmac_cp1h-xa40dt-d	1641
	sysmac_cp1h-xa40dt1-d	1642
	sysmac_cp1h-y20dt-d	1642
	sysmac_cp1l-el20dr-d	1643
	sysmac_cp1l-em30dr-d	1643
	sysmac_cp1l-em30dt-d	1644
	sysmac_cp1l-em30dt1-d	1644
	sysmac_cp1l-em40dr-d	1645
	sysmac_cp1l-em40dt-d	1646
	sysmac_cp1l-em40dt1-d	1646
	sysmac_cp1l-l10dr-a	1647
	sysmac_cp1l-l10dr-d	1647
	sysmac_cp1l-l10dt-a	1648
	sysmac_cp1l-l10dt-d	1648
	sysmac_cp1l-l10dt1-d	1649
	sysmac_cp1l-l14dr-a	1649
	sysmac_cp1l-l14dr-d	1650
	sysmac_cp1l-l14dt-a	1651
	sysmac_cp1l-l14dt-d	1651
	sysmac_cp1l-l14dt1-d	1652
sysmac_cp1l-l20dr-a	1652	

Vendor	Product	Page Number
Omron	sysmac_cp1l-l20dr-d	1653
	sysmac_cp1l-l20dt-a	1653
	sysmac_cp1l-l20dt-d	1654
	sysmac_cp1l-l20dt1-d	1654
	sysmac_cp1l-m30dr-a	1655
	sysmac_cp1l-m30dr-d	1656
	sysmac_cp1l-m30dt-a	1656
	sysmac_cp1l-m30dt-d	1657
	sysmac_cp1l-m30dt1-d	1657
	sysmac_cp1l-m40dr-a	1658
	sysmac_cp1l-m40dr-d	1658
	sysmac_cp1l-m40dt-a	1659
	sysmac_cp1l-m40dt-d	1659
	sysmac_cp1l-m40dt1-d	1660
	sysmac_cp1l-m60dr-a	1661
	sysmac_cp1l-m60dr-d	1661
	sysmac_cp1l-m60dt-a	1662
	sysmac_cp1l-m60dt-d	1662
	sysmac_cp1l-m60dt1-d	1663
	sysmac_cp2e-e14dr-a	1663
	sysmac_cp2e-e20dr-a	1664
	sysmac_cp2e-e30dr-a	1664
	sysmac_cp2e-e40dr-a	1665
	sysmac_cp2e-e60dr-a	1666
	sysmac_cp2e-n14dr-a	1666
	sysmac_cp2e-n14dr-d	1667
	sysmac_cp2e-n14dt-a	1667
	sysmac_cp2e-n14dt-d	1668
	sysmac_cp2e-n14dt1-d	1668
	sysmac_cp2e-n20dr-a	1669
	sysmac_cp2e-n20dr-d	1669
	sysmac_cp2e-n20dt-a	1670

Vendor	Product	Page Number
<b>Omron</b>	sysmac_cp2e-n20dt-d	1671
	sysmac_cp2e-n20dt1-d	1671
	sysmac_cp2e-n30dr-a	1672
	sysmac_cp2e-n30dr-d	1672
	sysmac_cp2e-n30dt-a	1673
	sysmac_cp2e-n30dt-d	1673
	sysmac_cp2e-n30dt1-d	1674
	sysmac_cp2e-n40dr-a	1674
	sysmac_cp2e-n40dr-d	1675
	sysmac_cp2e-n40dt-a	1676
	sysmac_cp2e-n40dt-d	1676
	sysmac_cp2e-n40dt1-d	1677
	sysmac_cp2e-n60dr-a	1677
	sysmac_cp2e-n60dr-d	1678
	sysmac_cp2e-n60dt-a	1678
	sysmac_cp2e-n60dt-d	1679
	sysmac_cp2e-n60dt1-d	1679
	sysmac_cp2e-s30dr-a	1680
	sysmac_cp2e-s30dt-d	1681
	sysmac_cp2e-s30dt1-d	1681
	sysmac_cp2e-s40dr-a	1682
	sysmac_cp2e-s40dt-d	1682
	sysmac_cp2e-s40dt1-d	1683
	sysmac_cp2e-s60dr-a	1683
	sysmac_cp2e-s60dt-d	1684
	sysmac_cp2e-s60dt1-d	1684
	sysmac_cs1w-drm21-v1	1685
	sysmac_cs1w-eip21	1686
	sysmac_cs1w-etn21	1686
	sysmac_cs1w-fln22	1687
	sysmac_cs1w-nc\[\]71	1687
	sysmac_cs1w-spu01-v2	1688

Vendor	Product	Page Number
<b>Omron</b>	sysmac_cs1w-spu02-v2	1688
<b>paradox</b>	ipr512	1689
<b>Samsung</b>	exynos	1689
	exynos_1080	1690
	exynos_2100	1691
	exynos_980	1691
	exynos_auto_t5123	1692
	exynos_modem_5123	1693
	exynos_modem_5300	1695
<b>sauter-controls</b>	ey-as525f001	1696
<b>silabs</b>	wireless_smart_ubiquitous_network_linux_bor der_router	1697
<b>Tenda</b>	ax3	1698
	g103	1698
	w20e	1698
<b>totolink</b>	a7100ru	1699
<b>Tp-link</b>	tl-mr3020	1699
<b>ui</b>	edgerouter_x	1699
<b>Operating System</b>		
<b>360</b>	d901_firmware	1701
<b>Apple</b>	macos	1701
<b>centralite</b>	pearl_firmware	1705
<b>Cisco</b>	ios	1705
	ios_xe	1998
	ios_xe_sd-wan	2229
<b>contiki-ng</b>	contiki-ng	2230
<b>Debian</b>	debian_linux	2231
<b>dek-1705_project</b>	dek-1705_firmware	2232
<b>Dell</b>	embedded_box_pc_3000_firmware	2233
<b>Dlink</b>	dir820la1_firmware	2233
<b>Fedoraproject</b>	fedora	2234
<b>Google</b>	android	2238
<b>hgiga</b>	powerstation_firmware	2317

Vendor	Product	Page Number
<b>HP</b>	integrated_lights-out_4	2318
	integrated_lights-out_5	2318
	integrated_lights-out_6	2318
<b>hpe</b>	arubaos-cx	2319
<b>jcgcn.com</b>	jhr-n916r_firmware	2321
<b>lancombg</b>	sa-wr915nd_firmware	2321
<b>Linux</b>	linux_kernel	2321
<b>Microsoft</b>	windows	2331
<b>Mikrotik</b>	routeros	2336
<b>Omron</b>	sysmac_cj2h-cpu64-eip_firmware	2336
	sysmac_cj2h-cpu64_firmware	2337
	sysmac_cj2h-cpu65-eip_firmware	2338
	sysmac_cj2h-cpu65_firmware	2338
	sysmac_cj2h-cpu66-eip_firmware	2339
	sysmac_cj2h-cpu66_firmware	2339
	sysmac_cj2h-cpu67-eip_firmware	2340
	sysmac_cj2h-cpu67_firmware	2340
	sysmac_cj2h-cpu68-eip_firmware	2341
	sysmac_cj2h-cpu68_firmware	2341
	sysmac_cj2m-cpu11_firmware	2342
	sysmac_cj2m-cpu12_firmware	2343
	sysmac_cj2m-cpu13_firmware	2343
	sysmac_cj2m-cpu14_firmware	2344
	sysmac_cj2m-cpu15_firmware	2344
	sysmac_cj2m-cpu31_firmware	2345
	sysmac_cj2m-cpu32_firmware	2345
	sysmac_cj2m-cpu33_firmware	2346
	sysmac_cj2m-cpu34_firmware	2346
	sysmac_cj2m-cpu35_firmware	2347
sysmac_cp1e-e10dr-a_firmware	2348	
sysmac_cp1e-e10dr-d_firmware	2348	
sysmac_cp1e-e10dt-a_firmware	2349	

Vendor	Product	Page Number
<b>Omron</b>	sysmac_cp1e-e10dt-d_firmware	2349
	sysmac_cp1e-e10dt1-a_firmware	2350
	sysmac_cp1e-e10dt1-d_firmware	2350
	sysmac_cp1e-e14dr-a_firmware	2351
	sysmac_cp1e-e14sdr-a_firmware	2351
	sysmac_cp1e-e20dr-a_firmware	2352
	sysmac_cp1e-e20sdr-a_firmware	2353
	sysmac_cp1e-e30dr-a_firmware	2353
	sysmac_cp1e-e30sdr-a_firmware	2354
	sysmac_cp1e-e40dr-a_firmware	2354
	sysmac_cp1e-e40sdr-a_firmware	2355
	sysmac_cp1e-e60sdr-a_firmware	2355
	sysmac_cp1e-na20dr-a_firmware	2356
	sysmac_cp1e-na20dt-d_firmware	2356
	sysmac_cp1e-na20dt1-d_firmware	2357
	sysmac_cp1h-x40dr-a_firmware	2358
	sysmac_cp1h-x40dt-d_firmware	2358
	sysmac_cp1h-x40dt1-d_firmware	2359
	sysmac_cp1h-xa40dr-a_firmware	2359
	sysmac_cp1h-xa40dt-d_firmware	2360
	sysmac_cp1h-xa40dt1-d_firmware	2360
	sysmac_cp1h-y20dt-d_firmware	2361
	sysmac_cp1l-el20dr-d_firmware	2361
	sysmac_cp1l-em30dr-d_firmware	2362
	sysmac_cp1l-em30dt-d_firmware	2363
	sysmac_cp1l-em30dt1-d_firmware	2363
	sysmac_cp1l-em40dr-d_firmware	2364
	sysmac_cp1l-em40dt-d_firmware	2364
	sysmac_cp1l-em40dt1-d_firmware	2365
	sysmac_cp1l-l10dr-a_firmware	2365
sysmac_cp1l-l10dr-d_firmware	2366	
sysmac_cp1l-l10dt-a_firmware	2366	

Vendor	Product	Page Number
<b>Omron</b>	sysmac_cp1l-l10dt-d_firmware	2367
	sysmac_cp1l-l10dt1-d_firmware	2368
	sysmac_cp1l-l14dr-a_firmware	2368
	sysmac_cp1l-l14dr-d_firmware	2369
	sysmac_cp1l-l14dt-a_firmware	2369
	sysmac_cp1l-l14dt-d_firmware	2370
	sysmac_cp1l-l14dt1-d_firmware	2370
	sysmac_cp1l-l20dr-a_firmware	2371
	sysmac_cp1l-l20dr-d_firmware	2371
	sysmac_cp1l-l20dt-a_firmware	2372
	sysmac_cp1l-l20dt-d_firmware	2373
	sysmac_cp1l-l20dt1-d_firmware	2373
	sysmac_cp1l-m30dr-a_firmware	2374
	sysmac_cp1l-m30dr-d_firmware	2374
	sysmac_cp1l-m30dt-a_firmware	2375
	sysmac_cp1l-m30dt-d_firmware	2375
	sysmac_cp1l-m30dt1-d_firmware	2376
	sysmac_cp1l-m40dr-a_firmware	2376
	sysmac_cp1l-m40dr-d_firmware	2377
	sysmac_cp1l-m40dt-a_firmware	2378
	sysmac_cp1l-m40dt-d_firmware	2378
	sysmac_cp1l-m40dt1-d_firmware	2379
	sysmac_cp1l-m60dr-a_firmware	2379
	sysmac_cp1l-m60dr-d_firmware	2380
	sysmac_cp1l-m60dt-a_firmware	2380
	sysmac_cp1l-m60dt-d_firmware	2381
	sysmac_cp1l-m60dt1-d_firmware	2381
	sysmac_cp2e-e14dr-a_firmware	2382
	sysmac_cp2e-e20dr-a_firmware	2383
	sysmac_cp2e-e30dr-a_firmware	2383
	sysmac_cp2e-e40dr-a_firmware	2384
	sysmac_cp2e-e60dr-a_firmware	2384

Vendor	Product	Page Number
<b>Omron</b>	sysmac_cp2e-n14dr-a_firmware	2385
	sysmac_cp2e-n14dr-d_firmware	2385
	sysmac_cp2e-n14dt-a_firmware	2386
	sysmac_cp2e-n14dt-d_firmware	2386
	sysmac_cp2e-n14dt1-d_firmware	2387
	sysmac_cp2e-n20dr-a_firmware	2388
	sysmac_cp2e-n20dr-d_firmware	2388
	sysmac_cp2e-n20dt-a_firmware	2389
	sysmac_cp2e-n20dt-d_firmware	2389
	sysmac_cp2e-n20dt1-d_firmware	2390
	sysmac_cp2e-n30dr-a_firmware	2390
	sysmac_cp2e-n30dr-d_firmware	2391
	sysmac_cp2e-n30dt-a_firmware	2391
	sysmac_cp2e-n30dt-d_firmware	2392
	sysmac_cp2e-n30dt1-d_firmware	2393
	sysmac_cp2e-n40dr-a_firmware	2393
	sysmac_cp2e-n40dr-d_firmware	2394
	sysmac_cp2e-n40dt-a_firmware	2394
	sysmac_cp2e-n40dt-d_firmware	2395
	sysmac_cp2e-n40dt1-d_firmware	2395
	sysmac_cp2e-n60dr-a_firmware	2396
	sysmac_cp2e-n60dr-d_firmware	2396
	sysmac_cp2e-n60dt-a_firmware	2397
	sysmac_cp2e-n60dt-d_firmware	2398
	sysmac_cp2e-n60dt1-d_firmware	2398
	sysmac_cp2e-s30dr-a_firmware	2399
	sysmac_cp2e-s30dt-d_firmware	2399
	sysmac_cp2e-s30dt1-d_firmware	2400
	sysmac_cp2e-s40dr-a_firmware	2400
	sysmac_cp2e-s40dt-d_firmware	2401
sysmac_cp2e-s40dt1-d_firmware	2401	
sysmac_cp2e-s60dr-a_firmware	2402	

Vendor	Product	Page Number
<b>Omron</b>	sysmac_cp2e-s60dt-d_firmware	2403
	sysmac_cp2e-s60dt1-d_firmware	2403
	sysmac_cs1w-drm21-v1_firmware	2404
	sysmac_cs1w-eip21_firmware	2404
	sysmac_cs1w-etn21_firmware	2405
	sysmac_cs1w-fln22_firmware	2405
	sysmac_cs1w-nc\[\]71_firmware	2406
	sysmac_cs1w-spu01-v2_firmware	2406
	sysmac_cs1w-spu02-v2_firmware	2407
<b>paradox</b>	ipr512_firmware	2408
<b>Redhat</b>	enterprise_linux	2408
	enterprise_linux_au	2411
	enterprise_linux_desktop	2412
	enterprise_linux_eus	2412
	enterprise_linux_for_ibm_z_systems	2414
	enterprise_linux_for_ibm_z_systems_eus	2415
	enterprise_linux_for_power_big_endian	2415
	enterprise_linux_for_power_little_endian	2416
	enterprise_linux_for_power_little_endian_eus	2417
	enterprise_linux_for_scientific_computing	2418
	enterprise_linux_server	2419
	enterprise_linux_server_au	2419
	enterprise_linux_server_for_power_little_endia n_update_services_for_sap_solutions	2420
	enterprise_linux_server_tus	2422
	enterprise_linux_server_update_services_for_s ap_solutions	2424
enterprise_linux_server_workstation	2424	
<b>Samsung</b>	android	2425
	exynos_1080_firmware	2431
	exynos_980_firmware	2432
	exynos_auto_t5123_firmware	2433
	exynos_firmware	2434

<b>Vendor</b>	<b>Product</b>	<b>Page Number</b>
<b>Samsung</b>	exynos_modem_5123_firmware	2435
	exynos_modem_5300_firmware	2436
<b>sauter-controls</b>	ey-as525f001_firmware	2437
<b>silabs</b>	wireless_smart_ubiquitous_network_linux_border_router_firmware	2439
<b>Tenda</b>	ax3_firmware	2439
	g103_firmware	2439
	w20e_firmware	2439
<b>totolink</b>	a7100ru_firmware	2440
<b>Tp-link</b>	tl-mr3020_firmware	2440
<b>ui</b>	edgerouter_x_firmware	2441

## Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
<b>Application</b>					
<b>Vendor: accesspressthemes</b>					
<b>Product: smart_logo_showcase_lite</b>					
Affected Version(s): 1.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.  <b>CVE ID : CVE-2023-0175</b>	N/A	A-ACC-SMAR-050423/1
Affected Version(s): 1.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform	N/A	A-ACC-SMAR-050423/2

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
			Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0175</b>		
Affected Version(s): 1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0175</b>	N/A	A-ACC-SMAR-050423/3
Affected Version(s): 1.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	N/A	A-ACC-SMAR-050423/4

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
			<b>CVE ID : CVE-2023-0175</b>		
Affected Version(s): 1.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0175</b>	N/A	A-ACC-SMAR-050423/5
Affected Version(s): 1.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0175</b>	N/A	A-ACC-SMAR-050423/6

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): 1.0.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.  <b>CVE ID : CVE-2023-0175</b>	N/A	A-ACC-SMAR-050423/7
Affected Version(s): 1.0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.  <b>CVE ID : CVE-2023-0175</b>	N/A	A-ACC-SMAR-050423/8
Affected Version(s): 1.0.8					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0175</b>	N/A	A-ACC-SMAR-050423/9
Affected Version(s): 1.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0175</b>	N/A	A-ACC-SMAR-050423/10
Affected Version(s): 1.1.0					
Improper Neutralization	20-Mar-2023	5.4	The Responsive Clients Logo Gallery	N/A	A-ACC-SMAR-050423/11

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0175</b>		
Affected Version(s): 1.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0175</b>	N/A	A-ACC-SMAR-050423/12
Affected Version(s): 1.1.2					
Improper Neutralization of Input	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9	N/A	A-ACC-SMAR-050423/13

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
During Web Page Generation ('Cross-site Scripting')			does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.  <b>CVE ID : CVE-2023-0175</b>		
Affected Version(s): 1.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.  <b>CVE ID : CVE-2023-0175</b>	N/A	A-ACC-SMAR-050423/14
Affected Version(s): 1.1.4					
Improper Neutralization of Input During Web Page	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its	N/A	A-ACC-SMAR-050423/15

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0175</b>		
Affected Version(s): 1.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0175</b>	N/A	A-ACC-SMAR-050423/16
Affected Version(s): 1.1.6					
Improper Neutralization of Input During Web Page Generation	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting	N/A	A-ACC-SMAR-050423/17

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 Scripting')			them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0175</b>		
Affected Version(s): 1.1.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0175</b>	N/A	A-ACC-SMAR-050423/18
Affected Version(s): 1.1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the	N/A	A-ACC-SMAR-050423/19

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
			shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0175</b>		
Affected Version(s): 1.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Responsive Clients Logo Gallery Plugin for WordPress plugin through 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0175</b>	N/A	A-ACC-SMAR-050423/20
<b>Product: wp_popup_banners</b>					
Affected Version(s): 1.0.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action.	N/A	A-ACC-WP_P-050423/21

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
			<b>CVE ID : CVE-2023-28661</b>		
Affected Version(s): 1.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/22
Affected Version(s): 1.0.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/23
Affected Version(s): 1.0.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/24

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): 1.0.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/25
Affected Version(s): 1.0.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/26
Affected Version(s): 1.0.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/27
Affected Version(s): 1.0.8					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/28
Affected Version(s): 1.0.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/29
Affected Version(s): 1.1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/30
Affected Version(s): 1.1.1					
Improper Neutralization	22-Mar-2023	8.8	The WP Popup Banners WordPress	N/A	A-ACC-WP_P-050423/31

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
ion of Special Elements used in an SQL Command ('SQL Injection')			Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>		
Affected Version(s): 1.1.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/32
Affected Version(s): 1.1.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/33
Affected Version(s): 1.1.4					
Improper Neutralization of Special	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an	N/A	A-ACC-WP_P-050423/34

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>		
Affected Version(s): 1.1.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/35
Affected Version(s): 1.1.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/36
Affected Version(s): 1.1.7					
Improper Neutralization of Special Elements used in an	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability	N/A	A-ACC-WP_P-050423/37

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>		
Affected Version(s): 1.1.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/38
Affected Version(s): 1.1.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/39
Affected Version(s): 1.2.0					
Improper Neutralization of Special Elements used in an SQL Command	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the	N/A	A-ACC-WP_P-050423/40

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			get_popup_data action. <b>CVE ID : CVE-2023-28661</b>		
Affected Version(s): 1.2.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/41
Affected Version(s): 1.2.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/42
Affected Version(s): 1.2.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action.	N/A	A-ACC-WP_P-050423/43

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
			<b>CVE ID : CVE-2023-28661</b>		
Affected Version(s): 1.2.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/44
Affected Version(s): 1.2.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action. <b>CVE ID : CVE-2023-28661</b>	N/A	A-ACC-WP_P-050423/45
<b>Vendor: admin_log_project</b>					
<b>Product: admin_log</b>					
Affected Version(s): * Up to (including) 1.50					
Cross-Site Request Forgery (CSRF)	20-Mar-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in David Gwyer Admin Log plugin <= 1.50 versions. <b>CVE ID : CVE-2023-23721</b>	N/A	A-ADM-ADMI-050423/46
<b>Vendor: Adobe</b>					

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
<b>Product: coldfusion</b>					
Affected Version(s): 2018					
Deserializa tion of Untrusted Data	23-Mar-2023	9.8	Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction.  <b>CVE ID : CVE-2023-26359</b>	<a href="https://helpx.adobe.com/security/products/coldfusion/psb23-25.html">https://hel px.adobe.co m/security /products/ coldfusion/ psb23- 25.html</a>	A-ADO-COLD-050423/47
Improper Access Control	23-Mar-2023	9.8	Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by an Improper Access Control vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction.  <b>CVE ID : CVE-2023-26360</b>	<a href="https://helpx.adobe.com/security/products/coldfusion/psb23-25.html">https://hel px.adobe.co m/security /products/ coldfusion/ psb23- 25.html</a>	A-ADO-COLD-050423/48
Improper Limitation of a Pathname to a	23-Mar-2023	4.9	Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by	<a href="https://helpx.adobe.com/security/products/coldfusion/">https://hel px.adobe.co m/security /products/ coldfusion/</a>	A-ADO-COLD-050423/49

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
Restricted Directory ('Path Traversal')			an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in Arbitrary file system read. Exploitation of this issue does not require user interaction, but does require administrator privileges. <b>CVE ID : CVE-2023-26361</b>	apsb23-25.html	
Affected Version(s): 2021					
Deserializa tion of Untrusted Data	23-Mar-2023	9.8	Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. <b>CVE ID : CVE-2023-26359</b>	<a href="https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html">https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html</a>	A-ADO-COLD-050423/50
Improper Access Control	23-Mar-2023	9.8	Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by an Improper Access Control vulnerability	<a href="https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html">https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html</a>	A-ADO-COLD-050423/51

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
			that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. <b>CVE ID : CVE-2023-26360</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	4.9	Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in Arbitrary file system read. Exploitation of this issue does not require user interaction, but does require administrator privileges. <b>CVE ID : CVE-2023-26361</b>	<a href="https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html">https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html</a>	A-ADO-COLD-050423/52
<b>Product: creative_cloud</b>					
Affected Version(s): * Up to (excluding) 5.10					
Untrusted Search Path	22-Mar-2023	7.8	Creative Cloud version 5.9.1 (and earlier) is affected by an Untrusted Search Path vulnerability that might allow attackers to execute their own programs, access unauthorized data	<a href="https://helpx.adobe.com/security/products/creative-cloud/apsb23-21.html">https://helpx.adobe.com/security/products/creative-cloud/apsb23-21.html</a>	A-ADO-CREA-050423/53

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
			files, or modify configuration in unexpected ways. If the application uses a search path to locate critical resources such as programs, then an attacker could modify that search path to point to a malicious program, which the targeted application would then execute. The problem extends to any type of critical resource that the application trusts.  <b>CVE ID : CVE-2023-26358</b>		
<b>Product: dimension</b>					
Affected Version(s): * Up to (excluding) 3.4.8					
Integer Overflow or Wraparound	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  <b>CVE ID : CVE-2023-25903</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/54
Access of Uninitialized Pointer	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an Access of	<a href="https://helpx.adobe.com/security/products/">https://helpx.adobe.com/security/products/</a>	A-ADO-DIME-050423/55

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
			<p>Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p><b>CVE ID : CVE-2023-26334</b></p>	dimension/apsb23-20.html	
Out-of-bounds Read	28-Mar-2023	7.8	<p>Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p><b>CVE ID : CVE-2023-26335</b></p>	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/56
Use After Free	28-Mar-2023	7.8	<p>Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current</p>	https://helpx.adobe.com/security/products/dimension/apsb23-20.html	A-ADO-DIME-050423/57

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26336</b>		
Out-of-bounds Write	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26337</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/58
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26338</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/59

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26339</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/60
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26340</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/61
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that	<a href="https://helpx.adobe.com/security/products/dimension/">https://helpx.adobe.com/security/products/dimension/</a>	A-ADO-DIME-050423/62

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
			could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26341</b>	apsb23-20.html	
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26342</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/63
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/64

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26343</b>		
Access of Uninitialized Pointer	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26344</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/65
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/66

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26345</b>		
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26346</b>	<a href="https://helpx.adobe.com/security/products/dimension/psb23-20.html">https://helpx.adobe.com/security/products/dimension/psb23-20.html</a>	A-ADO-DIME-050423/67
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	<a href="https://helpx.adobe.com/security/products/dimension/psb23-20.html">https://helpx.adobe.com/security/products/dimension/psb23-20.html</a>	A-ADO-DIME-050423/68

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-26348</b>		
Use After Free	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26349</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/69
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26350</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/70

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26351</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/71
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26352</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/72
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that	<a href="https://helpx.adobe.com/security/products/dimension/">https://helpx.adobe.com/security/products/dimension/</a>	A-ADO-DIME-050423/73

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26353</b>	apsb23-20.html	
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26354</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/74
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/75

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26355</b>		
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26356</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	A-ADO-DIME-050423/76
<b>Product: experience_manager</b>					
Affected Version(s): * Up to (excluding) 6.5.16.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (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	<a href="https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html">https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html</a>	A-ADO-EXPE-050423/77

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
			content may be executed within the context of the victim's browser. <b>CVE ID : CVE-2023-21615</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (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. <b>CVE ID : CVE-2023-21616</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html">https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html</a>	A-ADO-EXPE-050423/78
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (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. <b>CVE ID : CVE-2023-22252</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html">https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html</a>	A-ADO-EXPE-050423/79

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')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (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.  <b>CVE ID : CVE-2023-22253</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html</a>	A-ADO-EXPE-050423/80
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (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.  <b>CVE ID : CVE-2023-22254</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html</a>	A-ADO-EXPE-050423/81
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-	<a href="https://helpx.adobe.com/security/products/experience-manager/a">https://helpx.adobe.com/security/products/experience-manager/a</a>	A-ADO-EXPE-050423/82

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
			privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22256</b>	psb23-18.html	
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22257</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html</a>	A-ADO-EXPE-050423/83
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this	<a href="https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html</a>	A-ADO-EXPE-050423/84

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
			issue requires user interaction. <b>CVE ID : CVE-2023-22258</b>		
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22259</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/psb23-18.html</a>	A-ADO-EXPE-050423/85
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22260</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/psb23-18.html</a>	A-ADO-EXPE-050423/86
URL Redirection	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and	<a href="https://helpx.adobe.com">https://helpx.adobe.com</a>	A-ADO-EXPE-050423/87

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 to Untrusted Site ('Open Redirect')			earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22261</b>	m/security/products/experience-manager/a-psb23-18.html	
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22262</b>	https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html	A-ADO-EXPE-050423/88
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker	https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html	A-ADO-EXPE-050423/89

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
			could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22263</b>		
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22264</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html">https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html</a>	A-ADO-EXPE-050423/90
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this	<a href="https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html">https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html</a>	A-ADO-EXPE-050423/91

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
			issue requires user interaction. <b>CVE ID : CVE-2023-22265</b>		
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22266</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/psb23-18.html</a>	A-ADO-EXPE-050423/92
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (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. <b>CVE ID : CVE-2023-22269</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/psb23-18.html</a>	A-ADO-EXPE-050423/93

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
Inadequate Encryption Strength	22-Mar-2023	5.3	Experience Manager versions 6.5.15.0 (and earlier) are affected by a Weak Cryptography for Passwords vulnerability that can lead to a security feature bypass. A low-privileged attacker can exploit this in order to decrypt a user's password. The attack complexity is high since a successful exploitation requires to already have in possession this encrypted secret. <b>CVE ID : CVE-2023-22271</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html</a>	A-ADO-EXPE-050423/94
<b>Product: experience_manager_cloud_service</b>					
Affected Version(s): * Up to (excluding) 2023.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (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. <b>CVE ID : CVE-2023-21615</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html</a>	A-ADO-EXPE-050423/95
Improper Neutralization	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and	<a href="https://helpx.adobe.com">https://helpx.adobe.com</a>	A-ADO-EXPE-050423/96

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
ion of Input During Web Page Generation ('Cross-site Scripting')			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. <b>CVE ID : CVE-2023-21616</b>	m/security/products/experience-manager/a-psb23-18.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (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. <b>CVE ID : CVE-2023-22252</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html</a>	A-ADO-EXPE-050423/97
Improper Neutralization of Input During Web Page Generation	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (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	<a href="https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html</a>	A-ADO-EXPE-050423/98

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 Scripting')			referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. <b>CVE ID : CVE-2023-22253</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (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. <b>CVE ID : CVE-2023-22254</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/psb23-18.html</a>	A-ADO-EXPE-050423/99
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this	<a href="https://helpx.adobe.com/security/products/experience-manager/psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/psb23-18.html</a>	A-ADO-EXPE-050423/100

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
			issue requires user interaction. <b>CVE ID : CVE-2023-22256</b>		
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22257</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/psb23-18.html</a>	A-ADO-EXPE-050423/101
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22258</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/psb23-18.html</a>	A-ADO-EXPE-050423/102
URL Redirection	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and	<a href="https://helpx.adobe.com">https://helpx.adobe.com</a>	A-ADO-EXPE-050423/103

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n to Untrusted Site ('Open Redirect')			earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22259</b>	m/security/products/experience-manager/a-psb23-18.html	
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22260</b>	https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html	A-ADO-EXPE-050423/104
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker	https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html	A-ADO-EXPE-050423/105

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
			could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22261</b>		
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22262</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html">https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html</a>	A-ADO-EXPE-050423/106
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this	<a href="https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html">https://helpx.adobe.com/security/products/experience-manager/apsb23-18.html</a>	A-ADO-EXPE-050423/107

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
			issue requires user interaction. <b>CVE ID : CVE-2023-22263</b>		
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22264</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/psb23-18.html</a>	A-ADO-EXPE-050423/108
URL Redirection to Untrusted Site ('Open Redirect')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22265</b>	<a href="https://helpx.adobe.com/security/products/experience-manager/psb23-18.html">https://helpx.adobe.com/security/products/experience-manager/psb23-18.html</a>	A-ADO-EXPE-050423/109
URL Redirection	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (and	<a href="https://helpx.adobe.com">https://helpx.adobe.com</a>	A-ADO-EXPE-050423/110

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 to Untrusted Site ('Open Redirect')			earlier) are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. <b>CVE ID : CVE-2023-22266</b>	m/security/products/experience-manager/a-psb23-18.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	Experience Manager versions 6.5.15.0 (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. <b>CVE ID : CVE-2023-22269</b>	https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html	A-ADO-EXPE-050423/111
Inadequate Encryption Strength	22-Mar-2023	5.3	Experience Manager versions 6.5.15.0 (and earlier) are affected by a Weak Cryptography for Passwords vulnerability that can lead to a security feature bypass. A low-privileged attacker	https://helpx.adobe.com/security/products/experience-manager/a-psb23-18.html	A-ADO-EXPE-050423/112

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
			<p>can exploit this in order to decrypt a user's password. The attack complexity is high since a successful exploitation requires to already have in possession this encrypted secret.</p> <p><b>CVE ID : CVE-2023-22271</b></p>		
<b>Product: illustrator</b>					
Affected Version(s): * Up to (including) 26.5.2					
Improper Input Validation	22-Mar-2023	7.8	<p>Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p><b>CVE ID : CVE-2023-25859</b></p>	<p><a href="https://helpx.adobe.com/security/products/illustrator/psb23-19.html">https://helpx.adobe.com/security/products/illustrator/psb23-19.html</a></p>	A-ADO-ILLU-050423/113
Out-of-bounds Write	22-Mar-2023	7.8	<p>Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of</p>	<p><a href="https://helpx.adobe.com/security/products/illustrator/psb23-19.html">https://helpx.adobe.com/security/products/illustrator/psb23-19.html</a></p>	A-ADO-ILLU-050423/114

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
			this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-25860</b>		
Out-of-bounds Write	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-25861</b>	<a href="https://helpx.adobe.com/security/products/illustrator/psb23-19.html">https://helpx.adobe.com/security/products/illustrator/psb23-19.html</a>	A-ADO-ILLU-050423/115
Use After Free	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26426</b>	<a href="https://helpx.adobe.com/security/products/illustrator/psb23-19.html">https://helpx.adobe.com/security/products/illustrator/psb23-19.html</a>	A-ADO-ILLU-050423/116

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	22-Mar-2023	5.5	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-25862</b>	<a href="https://helpx.adobe.com/security/products/illustrator/apsb23-19.html">https://helpx.adobe.com/security/products/illustrator/apsb23-19.html</a>	A-ADO-ILLU-050423/117
Affected Version(s): From (including) 27.0.0 Up to (excluding) 27.3.1					
Improper Input Validation	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-25859</b>	<a href="https://helpx.adobe.com/security/products/illustrator/apsb23-19.html">https://helpx.adobe.com/security/products/illustrator/apsb23-19.html</a>	A-ADO-ILLU-050423/118
Out-of-bounds Write	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and	<a href="https://helpx.adobe.com/security">https://helpx.adobe.com/security</a>	A-ADO-ILLU-050423/119

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
			earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-25860</b>	/products/illustrator/psb23-19.html	
Out-of-bounds Write	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-25861</b>	<a href="https://helpx.adobe.com/security/products/illustrator/psb23-19.html">https://helpx.adobe.com/security/products/illustrator/psb23-19.html</a>	A-ADO-ILLU-050423/120
Use After Free	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires	<a href="https://helpx.adobe.com/security/products/illustrator/psb23-19.html">https://helpx.adobe.com/security/products/illustrator/psb23-19.html</a>	A-ADO-ILLU-050423/121

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26426</b>		
Out-of-bounds Read	22-Mar-2023	5.5	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-25862</b>	<a href="https://helpx.adobe.com/security/products/illustrator/apsb23-19.html">https://helpx.adobe.com/security/products/illustrator/apsb23-19.html</a>	A-ADO-ILLU-050423/122
<b>Vendor: air_cargo_management_system_project</b>					
<b>Product: air_cargo_management_system</b>					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	A vulnerability was found in SourceCodester Air Cargo Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file admin/transactions/update_status.php of the component GET Parameter Handler. The manipulation of	N/A	A-AIR-AIR_-050423/123

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
			<p>the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223556.</p> <p><b>CVE ID : CVE-2023-1564</b></p>		
<b>Vendor: alphaware_-_simple_e-commerce_system_project</b>					
<b>Product: alphaware_-_simple_e-commerce_system</b>					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Mar-2023	9.8	<p>A vulnerability was found in SourceCodester Alphaware Simple E-Commerce System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file function/edit_customer.php. The manipulation of the argument firstname/mi/lastname with the input a'RLIKE SLEEP(5) AND 'dAbu'='dAbu leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-223406 is the identifier assigned to this vulnerability.</p>	N/A	A-ALP-ALPH-050423/124

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
			<b>CVE ID : CVE-2023-1502</b>		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Mar-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Alphaware Simple E-Commerce System 1.0. This affects an unknown part of the file admin/admin_index.php. The manipulation of the argument username/password with the input admin' AND (SELECT 8062 FROM (SELECT(SLEEP(5))) meUD)-- hLiX leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223407. <b>CVE ID : CVE-2023-1503</b>	N/A	A-ALP-ALPH-050423/125
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Mar-2023	9.8	A vulnerability classified as critical was found in SourceCodester Alphaware Simple E-Commerce System 1.0. This vulnerability affects unknown code. The manipulation of the argument email/password with the input	N/A	A-ALP-ALPH-050423/126

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
			test1%40test.com ' AND (SELECT 6077 FROM (SELECT(SLEEP(5)))d ltn) AND 'PhRa'='PhRa leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223408. <b>CVE ID : CVE-2023-1504</b>		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Mar-2023	9.8	An issue was discovered in Alphaware - Simple E-Commerce System v1.0. There is a SQL injection that can directly issue instructions to the background database system via /alphaware/details.php?id. <b>CVE ID : CVE-2023-26905</b>	N/A	A-ALP-ALPH-050423/127
<b>Vendor: altanic</b>					
<b>Product: no_api_amazon_affiliate</b>					
Affected Version(s): * Up to (including) 4.2.2					
Improper Neutralization of Input During Web Page Generation	20-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Altanic No API Amazon Affiliate plugin <= 4.2.2 versions.	N/A	A-ALT-NO_A-050423/128

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 Scripting')			<b>CVE ID : CVE-2023-22680</b>		
<b>Vendor: amano</b>					
<b>Product: xoffice</b>					
Affected Version(s): 7.1.3879					
Files or Directories Accessible to External Parties	28-Mar-2023	7.5	amano Xparc parking solutions 7.1.3879 was discovered to be vulnerable to local file inclusion. <b>CVE ID : CVE-2023-23330</b>	N/A	A-AMA-XOFF-050423/129
<b>Vendor: ansible-semaphore</b>					
<b>Product: ansible_semaphore</b>					
Affected Version(s): * Up to (excluding) 2.8.89					
Improper Authentication	18-Mar-2023	9.8	api/auth.go in Ansible Semaphore before 2.8.89 mishandles authentication. <b>CVE ID : CVE-2023-28609</b>	<a href="https://github.com/ansible-semaphore/semaphore/commit/3e4a62b7f2b1ef0660c9fb839818a53c80a5a8b1">https://github.com/ansible-semaphore/semaphore/commit/3e4a62b7f2b1ef0660c9fb839818a53c80a5a8b1</a>	A-ANS-ANSI-050423/130
<b>Vendor: answer</b>					
<b>Product: answer</b>					
Affected Version(s): * Up to (excluding) 1.0.6					
Authentication Bypass by Capture-replay	21-Mar-2023	9.8	Authentication Bypass by Capture-replay in GitHub repository answerdev/answer prior to 1.0.6. <b>CVE ID : CVE-2023-1537</b>	<a href="https://github.com/answerdev/answer/commit/813ad0b9894673b1bdd489a2e9ab60a44fe990af">https://github.com/answerdev/answer/commit/813ad0b9894673b1bdd489a2e9ab60a44fe990af</a> , <a href="https://hu">https://hu</a>	A-ANS-ANSW-050423/131

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
				ntr.dev/bo unties/171 cde18- a447-446c- a9ab- 297953ad9 b86	
Insufficient Session Expiration	21-Mar-2023	8.8	Insufficient Session Expiration in GitHub repository answerdev/answer prior to 1.0.6. <b>CVE ID : CVE-2023-1543</b>	https://github.com/answerdev/answer/commit/cd742b75605c99776f32d271c0a60e0f468e181c, https://ntr.dev/bo unties/f82388d6- dfc3-4fbc- bea6- eb40cf5b2 683	A-ANS-ANSW-050423/132
N/A	21-Mar-2023	5.4	Business Logic Errors in GitHub repository answerdev/answer prior to 1.0.6. <b>CVE ID : CVE-2023-1542</b>	https://github.com/answerdev/answer/commit/4ca2429d190a6e614f5bbee1173c80a7cfffcc568, https://ntr.dev/bo unties/d947417c- 5a12-407a- 9a2f- fa696f6512 6f	A-ANS-ANSW-050423/133

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
Observable Discrepancy	21-Mar-2023	5.3	Observable Timing Discrepancy in GitHub repository answerdev/answer prior to 1.0.6. <b>CVE ID : CVE-2023-1538</b>	<a href="https://github.com/answerdev/answer/commit/813ad0b9894673b1bdd489a2e9ab60a44fe990af">https://github.com/answerdev/answer/commit/813ad0b9894673b1bdd489a2e9ab60a44fe990af</a> , <a href="https://huntr.dev/bounties/ac0271eb-660f-4966-8b57-4bc660a9a1a0">https://huntr.dev/bounties/ac0271eb-660f-4966-8b57-4bc660a9a1a0</a>	A-ANS-ANSW-050423/134
Improper Restriction of Excessive Authentication Attempts	21-Mar-2023	5.3	Guessable CAPTCHA in GitHub repository answerdev/answer prior to 1.0.6. <b>CVE ID : CVE-2023-1539</b>	<a href="https://huntr.dev/bounties/b4df67f4-14ea-4051-97d4-26690c979a28">https://huntr.dev/bounties/b4df67f4-14ea-4051-97d4-26690c979a28</a> , <a href="https://github.com/answerdev/answer/commit/813ad0b9894673b1bdd489a2e9ab60a44fe990af">https://github.com/answerdev/answer/commit/813ad0b9894673b1bdd489a2e9ab60a44fe990af</a>	A-ANS-ANSW-050423/135
Observable Discrepancy	21-Mar-2023	5.3	Observable Response Discrepancy in GitHub repository answerdev/answer prior to 1.0.6. <b>CVE ID : CVE-2023-1540</b>	<a href="https://huntr.dev/bounties/d8d6c259-a0f2-4209-a3b0-ecbf3eb092f4">https://huntr.dev/bounties/d8d6c259-a0f2-4209-a3b0-ecbf3eb092f4</a> , <a href="https://github.com/answerdev/answer/commit/813ad0b9894673b1bdd489a2e9ab60a44fe990af">https://github.com/answerdev/answer/commit/813ad0b9894673b1bdd489a2e9ab60a44fe990af</a>	A-ANS-ANSW-050423/136

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
				hub.com/answerdev/answer/commit/1de3ec27e50ba7389c9449c59e8ea3a37a908ee4	
N/A	21-Mar-2023	3.8	Business Logic Errors in GitHub repository answerdev/answer prior to 1.0.6. <b>CVE ID : CVE-2023-1541</b>	https://github.com/answerdev/answer/commit/15390adbfc5fd37af4661f992f8873ae5a6b840, https://huntr.dev/bounties/8fd891c6-b04e-4dac-818f-9ea30861cd92	A-ANS-ANSW-050423/137
Affected Version(s): * Up to (excluding) 1.0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.7. <b>CVE ID : CVE-2023-1535</b>	https://huntr.dev/bounties/4d4b0caab6d8c-4574-ae7e-e9ef5e2e1a40, https://github.com/answerdev/answer/commit/c3743bad4f2a69f69f8f1e1e5b4b6524fc03da25	A-ANS-ANSW-050423/138

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')	21-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.7. <b>CVE ID : CVE-2023-1536</b>	<a href="https://huntr.dev/bounties/538207f4-f805-419a-a314-51716643f05e">https://huntr.dev/bounties/538207f4-f805-419a-a314-51716643f05e</a> , <a href="https://github.com/answerdev/answer/commit/c3743bad4f2a69f69f8f1e1e5b4b6524fc03da25">https://github.com/answerdev/answer/commit/c3743bad4f2a69f69f8f1e1e5b4b6524fc03da25</a>	A-ANS-ANSW-050423/139

**Vendor: Apache**

**Product: fineract**

Affected Version(s): From (including) 1.4.0 Up to (including) 1.8.2

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Mar-2023	6.3	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Software Foundation apache fineract. Authorized users may be able to exploit this for limited impact on components. This issue affects apache fineract: from 1.4 through 1.8.2. <b>CVE ID : CVE-2023-25197</b>	<a href="https://lists.apache.org/thread/v0q9x86sx6f6l2nzm3y9qlng04">https://lists.apache.org/thread/v0q9x86sx6f6l2nzm3y9qlng04</a>	A-APA-FINE-050423/140
Improper Neutralization of Special	28-Mar-2023	4.3	Improper Neutralization of Special Elements used in an SQL Command	<a href="https://lists.apache.org/thread/m9x3vpn3">https://lists.apache.org/thread/m9x3vpn3</a>	A-APA-FINE-050423/141

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			('SQL Injection') vulnerability in Apache Software Foundation Apache Fineract. Authorized users may be able to change or add data in certain components. This issue affects Apache Fineract: from 1.4 through 1.8.2. <b>CVE ID : CVE-2023-25196</b>	bry4fympk zxnnz4qx0 oc0w8m	
Affected Version(s): From (including) 1.4.0 Up to (including) 1.8.3					
Server-Side Request Forgery (SSRF)	28-Mar-2023	8.1	Server-Side Request Forgery (SSRF) vulnerability in Apache Software Foundation Apache Fineract. Authorized users with limited permissions can gain access to server and may be able to use server for any outbound traffic. This issue affects Apache Fineract: from 1.4 through 1.8.3. <b>CVE ID : CVE-2023-25195</b>	<a href="https://lists.apache.org/thread/m58fdjmtkfp9h4c0r4l48rv995w3qhb6">https://lists.apache.org/thread/m58fdjmtkfp9h4c0r4l48rv995w3qhb6</a>	A-APA-FINE-050423/142
<b>Product: inlong</b>					
Affected Version(s): From (including) 1.1.0 Up to (including) 1.5.0					
Deserialization of Untrusted Data	27-Mar-2023	8.8	Deserialization of Untrusted Data vulnerability in Apache Software Foundation Apache InLong. It could be triggered by authenticated users of InLong, you could	<a href="https://lists.apache.org/thread/xbvtjw9bwzgb09fp1by8o3p49nf59xzt">https://lists.apache.org/thread/xbvtjw9bwzgb09fp1by8o3p49nf59xzt</a>	A-APA-INLO-050423/143

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
			<p>refer to [1] to know more about this vulnerability. This issue affects Apache InLong: from 1.1.0 through 1.5.0. Users are advised to upgrade to Apache InLong's latest version or cherry-pick [2] to solve it. [1]</p> <p><a href="https://programmer.help/blogs/jdbc-deserialization-vulnerability-learning.html">https://programmer.help/blogs/jdbc-deserialization-vulnerability-learning.html</a></p> <p><a href="https://programmer.help/blogs/jdbc-deserialization-vulnerability-learning.html">https://programmer.help/blogs/jdbc-deserialization-vulnerability-learning.html</a> [2]</p> <p><a href="https://github.com/apache/inlong/pull/7422">https://github.com/apache/inlong/pull/7422</a></p> <p><a href="https://github.com/apache/inlong/pull/7422">https://github.com/apache/inlong/pull/7422</a></p> <p><b>CVE ID : CVE-2023-27296</b></p>		
<b>Product: sling_resource_merger</b>					
Affected Version(s): From (including) 1.2.0 Up to (excluding) 1.4.2					
Excessive Iteration	20-Mar-2023	7.5	<p>Excessive Iteration vulnerability in Apache Software Foundation Apache Sling Resource Merger. This issue affects Apache Sling Resource Merger: from 1.2.0 before 1.4.2.</p>	<p><a href="https://lists.apache.org/thread/xpcco1y88ldss5hgmvogsf6h373515zb">https://lists.apache.org/thread/xpcco1y88ldss5hgmvogsf6h373515zb</a></p>	A-APA-SLIN-050423/144

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
			<b>CVE ID : CVE-2023-26513</b>		
<b>Product: tomcat</b>					
Affected Version(s): 11.0.0					
Unprotected Transport of Credentials	22-Mar-2023	4.3	When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Apache Tomcat 11.0.0-M1 to 11.0.0-M2, 10.1.0-M1 to 10.1.5, 9.0.0-M1 to 9.0.71 and 8.5.0 to 8.5.85 did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel.  <b>CVE ID : CVE-2023-28708</b>	<a href="https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67">https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67</a>	A-APA-TOMC-050423/145
Affected Version(s): From (excluding) 10.1.0 Up to (excluding) 10.1.6					
Unprotected Transport of Credentials	22-Mar-2023	4.3	When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Apache Tomcat 11.0.0-M1 to 11.0.0-M2, 10.1.0-M1 to 10.1.5, 9.0.0-M1 to 9.0.71 and 8.5.0 to 8.5.85 did not include the secure attribute.	<a href="https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67">https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67</a>	A-APA-TOMC-050423/146

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
			This could result in the user agent transmitting the session cookie over an insecure channel. <b>CVE ID : CVE-2023-28708</b>		
Affected Version(s): From (excluding) 9.0.0 Up to (excluding) 9.0.72					
Unprotected Transport of Credentials	22-Mar-2023	4.3	When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Apache Tomcat 11.0.0-M1 to 11.0.0-M2, 10.1.0-M1 to 10.1.5, 9.0.0-M1 to 9.0.71 and 8.5.0 to 8.5.85 did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel. <b>CVE ID : CVE-2023-28708</b>	<a href="https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67">https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67</a>	A-APA-TOMC-050423/147
Affected Version(s): From (including) 8.5.0 Up to (excluding) 8.5.86					
Unprotected Transport of Credentials	22-Mar-2023	4.3	When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Apache Tomcat 11.0.0-M1 to 11.0.0-M2, 10.1.0-M1	<a href="https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67">https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67</a>	A-APA-TOMC-050423/148

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to 10.1.5, 9.0.0-M1 to 9.0.71 and 8.5.0 to 8.5.85 did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel. <b>CVE ID : CVE-2023-28708</b>		

**Vendor: apiman**

**Product: apiman**

Affected Version(s): 3.0.0

Missing Authorization	27-Mar-2023	3.1	Apiman is a flexible and open source API Management platform. Due to a missing permissions check, an attacker with an authenticated Apiman Manager account may be able to gain access to API keys they do not have permission for if they correctly guess the URL, which includes Organisation ID, Client ID, and Client Version of the targeted non-permitted resource. While not trivial to exploit, it could be achieved by brute-forcing or guessing common names. Access to the non-permitted API Keys could allow use of other users' resources without their	<a href="https://github.com/apiman/apiman/security/advisories/GHSA-m6f8-hjrv-mw5f">https://github.com/apiman/apiman/security/advisories/GHSA-m6f8-hjrv-mw5f</a> , <a href="https://www.apiman.io/blog/potential-permissions-bypass-disclosure/">https://www.apiman.io/blog/potential-permissions-bypass-disclosure/</a>	A-API-APIM-050423/149
-----------------------	-------------	-----	---	--	-----------------------

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
			<p>permission (depending on the specifics of configuration, such as whether an API key is the only form of security). Apiman 3.1.0.Final resolved this issue. Users are advised to upgrade. The only known workaround is to restrict account access.</p> <p><b>CVE ID : CVE-2023-28640</b></p>		

**Vendor: Arubanetworks**

**Product: clearpass\_policy\_manager**

Affected Version(s): 6.11.0

N/A	22-Mar-2023	9.8	<p>A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to create arbitrary users on the platform. A successful exploit allows an attacker to achieve total cluster compromise.</p> <p><b>CVE ID : CVE-2023-25589</b></p>	<p><a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a></p>	A-ARU-CLEA-050423/150
Incorrect Authorization	22-Mar-2023	8.8	<p>A vulnerability in the web-based management interface of ClearPass Policy Manager allows an attacker with read-only privileges to perform actions that</p>	<p><a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a></p>	A-ARU-CLEA-050423/151

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
			change the state of the ClearPass Policy Manager instance. Successful exploitation of this vulnerability allows an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform. <b>CVE ID : CVE-2023-25594</b>		
Improper Privilege Management	22-Mar-2023	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance. <b>CVE ID : CVE-2023-25590</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/152
N/A	22-Mar-2023	6.5	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow a remote attacker authenticated with low privileges to access sensitive	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/153

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further privileges on the ClearPass instance. <b>CVE ID : CVE-2023-25591</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. <b>CVE ID : CVE-2023-25592</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/154
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/155

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
			script code in a victim's browser in the context of the affected interface. <b>CVE ID : CVE-2023-25593</b>		
N/A	22-Mar-2023	5.5	A vulnerability exists in the ClearPass OnGuard Ubuntu agent that allows for an attacker with local Ubuntu instance access to potentially obtain sensitive information. Successful Exploitation of this vulnerability allows an attacker to retrieve information that is of a sensitive nature to the ClearPass/OnGuard environment. <b>CVE ID : CVE-2023-25595</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/156
Cleartext Storage of Sensitive Information	22-Mar-2023	4.9	A vulnerability exists in ClearPass Policy Manager that allows for an attacker with administrative privileges to access sensitive information in a cleartext format. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further access to network services supported by	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/157

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ClearPass Policy Manager. <b>CVE ID : CVE-2023-25596</b>		
Affected Version(s): 6.11.1					
N/A	22-Mar-2023	9.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to create arbitrary users on the platform. A successful exploit allows an attacker to achieve total cluster compromise. <b>CVE ID : CVE-2023-25589</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/158
Incorrect Authorization	22-Mar-2023	8.8	A vulnerability in the web-based management interface of ClearPass Policy Manager allows an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of this vulnerability allows an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/159

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
			authorization on the platform. <b>CVE ID : CVE-2023-25594</b>		
Improper Privilege Management	22-Mar-2023	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance. <b>CVE ID : CVE-2023-25590</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/160
N/A	22-Mar-2023	6.5	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow a remote attacker authenticated with low privileges to access sensitive information. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further privileges on the ClearPass instance. <b>CVE ID : CVE-2023-25591</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/161
Improper Neutralizat	22-Mar-2023	6.1	Vulnerabilities within the web-based	<a href="https://www.arubanet">https://www.arubanet</a>	A-ARU-CLEA-050423/162

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
ion of Input During Web Page Generation ('Cross-site Scripting')			management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. <b>CVE ID : CVE-2023-25592</b>	works.com/assets/alert/ARUBA-PSA-2023-003.txt	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. <b>CVE ID : CVE-2023-25593</b>	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt	A-ARU-CLEA-050423/163
N/A	22-Mar-2023	5.5	A vulnerability exists in the ClearPass OnGuard Ubuntu agent that allows for an attacker with local Ubuntu instance access to potentially	https://www.arubanetworks.com/assets/alert/ARUBA-	A-ARU-CLEA-050423/164

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
			obtain sensitive information. Successful Exploitation of this vulnerability allows an attacker to retrieve information that is of a sensitive nature to the ClearPass/OnGuard environment. <b>CVE ID : CVE-2023-25595</b>	PSA-2023-003.txt	
Cleartext Storage of Sensitive Information	22-Mar-2023	4.9	A vulnerability exists in ClearPass Policy Manager that allows for an attacker with administrative privileges to access sensitive information in a cleartext format. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further access to network services supported by ClearPass Policy Manager. <b>CVE ID : CVE-2023-25596</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/165
Affected Version(s): From (including) 6.10.0 Up to (including) 6.10.8					
N/A	22-Mar-2023	9.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to create arbitrary users	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/166

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
			on the platform. A successful exploit allows an attacker to achieve total cluster compromise. <b>CVE ID : CVE-2023-25589</b>		
Incorrect Authorization	22-Mar-2023	8.8	A vulnerability in the web-based management interface of ClearPass Policy Manager allows an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of this vulnerability allows an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform. <b>CVE ID : CVE-2023-25594</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/167
Improper Privilege Management	22-Mar-2023	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/168

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary code with root level privileges on the Linux instance. <b>CVE ID : CVE-2023-25590</b>		
N/A	22-Mar-2023	6.5	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow a remote attacker authenticated with low privileges to access sensitive information. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further privileges on the ClearPass instance. <b>CVE ID : CVE-2023-25591</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/169
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/170

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the context of the affected interface. <b>CVE ID : CVE-2023-25592</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. <b>CVE ID : CVE-2023-25593</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/171
N/A	22-Mar-2023	5.5	A vulnerability exists in the ClearPass OnGuard Ubuntu agent that allows for an attacker with local Ubuntu instance access to potentially obtain sensitive information. Successful Exploitation of this vulnerability allows an attacker to retrieve information that is of a sensitive nature to the ClearPass/OnGuard environment.	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/172

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
			<b>CVE ID : CVE-2023-25595</b>		
Cleartext Storage of Sensitive Information	22-Mar-2023	4.9	A vulnerability exists in ClearPass Policy Manager that allows for an attacker with administrative privileges to access sensitive information in a cleartext format. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further access to network services supported by ClearPass Policy Manager. <b>CVE ID : CVE-2023-25596</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/173
Affected Version(s): From (including) 6.9.0 Up to (including) 6.9.13					
N/A	22-Mar-2023	9.8	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to create arbitrary users on the platform. A successful exploit allows an attacker to achieve total cluster compromise. <b>CVE ID : CVE-2023-25589</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/174
Incorrect Authorization	22-Mar-2023	8.8	A vulnerability in the web-based management interface of ClearPass Policy	<a href="https://www.arubanetworks.com/assets/ale">https://www.arubanetworks.com/assets/ale</a>	A-ARU-CLEA-050423/175

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
			<p>Manager allows an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of this vulnerability allows an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform.</p> <p><b>CVE ID : CVE-2023-25594</b></p>	rt/ARUBA-PSA-2023-003.txt	
Improper Privilege Management	22-Mar-2023	7.8	<p>A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance.</p> <p><b>CVE ID : CVE-2023-25590</b></p>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/176
N/A	22-Mar-2023	6.5	<p>A vulnerability in the web-based management interface of ClearPass Policy Manager could allow a</p>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/177

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker authenticated with low privileges to access sensitive information. A successful exploit allows an attacker to retrieve information which could be used to potentially gain further privileges on the ClearPass instance. <b>CVE ID : CVE-2023-25591</b>	PSA-2023-003.txt	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. <b>CVE ID : CVE-2023-25592</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/178
Improper Neutralization of Input During Web Page Generation	22-Mar-2023	6.1	Vulnerabilities within the web-based management interface of ClearPass Policy Manager could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/179

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 Scripting')			user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. <b>CVE ID : CVE-2023-25593</b>		
N/A	22-Mar-2023	5.5	A vulnerability exists in the ClearPass OnGuard Ubuntu agent that allows for an attacker with local Ubuntu instance access to potentially obtain sensitive information. Successful Exploitation of this vulnerability allows an attacker to retrieve information that is of a sensitive nature to the ClearPass/OnGuard environment. <b>CVE ID : CVE-2023-25595</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/180
Cleartext Storage of Sensitive Information	22-Mar-2023	4.9	A vulnerability exists in ClearPass Policy Manager that allows for an attacker with administrative privileges to access sensitive information in a cleartext format. A successful exploit allows an attacker to retrieve information which could be used to potentially gain	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	A-ARU-CLEA-050423/181

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
			further access to network services supported by ClearPass Policy Manager. <b>CVE ID : CVE-2023-25596</b>		

**Vendor: askoc**

**Product: web\_report\_system**

Affected Version(s): \* Up to (excluding) 23.03.10

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in As Koc Energy Web Report System allows SQL Injection.This issue affects Web Report System: before 23.03.10. <b>CVE ID : CVE-2023-1050</b>	N/A	A-ASK-WEB_-050423/182
--	-------------	-----	--	-----	-----------------------

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in As Koc Energy Web Report System allows Reflected XSS.This issue affects Web Report System: before 23.03.10. <b>CVE ID : CVE-2023-1051</b>	N/A	A-ASK-WEB_-050423/183
--	-------------	-----	--	-----	-----------------------

**Vendor: automatic\_question\_paper\_generator\_system\_project**

**Product: automatic\_question\_paper\_generator\_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): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability has been found in SourceCodester Automatic Question Paper Generator System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file admin/courses/view_course.php of the component GET Parameter Handler. The manipulation of the argument id 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-223285 was assigned to this vulnerability. <b>CVE ID : CVE-2023-1441</b>	N/A	A-AUT-AUTO-050423/184
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability classified as critical was found in SourceCodester Automatic Question Paper Generator System 1.0. This vulnerability affects unknown code of the file users/question_papers/manage_question_paper.php of the component GET	N/A	A-AUT-AUTO-050423/185

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
			Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223336. <b>CVE ID : CVE-2023-1474</b>		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Automatic Question Paper Generator System 1.0. This affects an unknown part of the file classes/Users.php?f=save_ruser. The manipulation of the argument id/email leads to sql injection. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-223659. <b>CVE ID : CVE-2023-1591</b>	N/A	A-AUT-AUTO-050423/186
Improper Neutralization of Special Elements used in an SQL Command	23-Mar-2023	9.8	A vulnerability classified as critical was found in SourceCodester Automatic Question Paper Generator System 1.0. This vulnerability affects	N/A	A-AUT-AUTO-050423/187

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			<p>unknown code of the file admin/courses/view_class.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The identifier of this vulnerability is VDB-223660.</p> <p><b>CVE ID : CVE-2023-1592</b></p>		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	8.8	<p>A vulnerability, which was classified as critical, was found in SourceCodester Automatic Question Paper Generator System 1.0. Affected is an unknown function of the file users/user/manage_user.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223284.</p> <p><b>CVE ID : CVE-2023-1440</b></p>	N/A	A-AUT-AUTO-050423/188

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')	23-Mar-2023	6.1	A vulnerability, which was classified as problematic, has been found in SourceCodester Automatic Question Paper Generator System 1.0. This issue affects some unknown processing of the file classes/Master.php?f=save_class. The manipulation of the argument description leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-223661 was assigned to this vulnerability. <b>CVE ID : CVE-2023-1593</b>	N/A	A-AUT-AUTO-050423/189
<b>Vendor: Aver</b>					
<b>Product: ptzapp_2</b>					
Affected Version(s): * Up to (excluding) 2.0.1051.53					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Mar-2023	7.5	Aver Information Inc PTZApp2 v20.01044.48 allows attackers to access sensitive files via a crafted GET request. <b>CVE ID : CVE-2023-27055</b>	N/A	A-AVE-PTZA-050423/190
<b>Vendor: aveva</b>					
<b>Product: aveva_plant_scada</b>					
Affected Version(s): 2020r2					
Improper Authorization	16-Mar-2023	9.8	The listed versions of AVEVA Plant SCADA and AVEVA Telemetry	N/A	A-AVE-AVEV-050423/191

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
			Server are vulnerable to an improper authorization exploit which could allow an unauthenticated user to remotely read data, cause denial of service, and tamper with alarm states. <b>CVE ID : CVE-2023-1256</b>		
Affected Version(s): 2023					
Improper Authorization	16-Mar-2023	9.8	The listed versions of AVEVA Plant SCADA and AVEVA Telemetry Server are vulnerable to an improper authorization exploit which could allow an unauthenticated user to remotely read data, cause denial of service, and tamper with alarm states. <b>CVE ID : CVE-2023-1256</b>	N/A	A-AVE-AVEV-050423/192
<b>Product: telemetry_server</b>					
Affected Version(s): 2020r2					
Improper Authorization	16-Mar-2023	9.8	The listed versions of AVEVA Plant SCADA and AVEVA Telemetry Server are vulnerable to an improper authorization exploit which could allow an unauthenticated user to remotely read data, cause denial of service, and tamper with alarm states.	N/A	A-AVE-TELE-050423/193

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
			<b>CVE ID : CVE-2023-1256</b>		
<b>Vendor: awsm</b>					
<b>Product: embed_any_document</b>					
Affected Version(s): * Up to (including) 2.7.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Unrestricted Upload of File with Dangerous Type vulnerability in AwsM Innovations Embed Any Document – Embed PDF, Word, PowerPoint and Excel Files allows Stored XSS via upload of SVG and HTML files. This issue affects Embed Any Document – Embed PDF, Word, PowerPoint and Excel Files plugin <= 2.7.1 versions. <b>CVE ID : CVE-2023-23707</b>	N/A	A-AWS-EMBE-050423/194
<b>Vendor: Basercms</b>					
<b>Product: basercms</b>					
Affected Version(s): * Up to (excluding) 4.7.5					
Unrestricted Upload of File with Dangerous Type	23-Mar-2023	9.8	basercMS is a Content Management system. Prior to version 4.7.5, there is a Remote Code Execution (RCE) Vulnerability in the management system of basercMS. Version 4.7.5 contains a patch.	<a href="https://github.com/basercms/basercms/commit/60f83054d8131b0ace60716cec7e629b5eb3a8">https://github.com/basercms/basercms/commit/60f83054d8131b0ace60716cec7e629b5eb3a8</a>	A-BAS-BASE-050423/195

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-25654</b>	f0, https://github.com/baserproject/basercms/commit/002886be0998c74c386e04f0b43688a8a45d7a96	
Unrestricted Upload of File with Dangerous Type	23-Mar-2023	9.8	baserCMS is a Content Management system. Prior to version 4.7.5, any file may be uploaded on the management system of baserCMS. Version 4.7.5 contains a patch. <b>CVE ID : CVE-2023-25655</b>	https://github.com/baserproject/basercms/commit/9297629983ed908c7f51bf61a0231dde91404ebd, https://github.com/baserproject/basercms/commit/922025a98b0e697ab78f6a785a004e0729aa9100	A-BAS-BASE-050423/196
<b>Vendor: basixonline</b>					
<b>Product: nex-forms</b>					
Affected Version(s): * Up to (excluding) 8.3.3					
Improper Neutralization of Input During Web Page Generation	27-Mar-2023	5.4	The NEX-Forms WordPress plugin before 8.3.3 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where	N/A	A-BAS-NEX--050423/197

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 Scripting')			the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks <b>CVE ID : CVE-2023-0272</b>		

**Vendor: booking-wp-plugin**

**Product: bookly**

Affected Version(s): \* Up to (excluding) 21.5.1

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Mar-2023	6.1	The Bookly plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the full name value in versions up to, and including, 21.5 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. <b>CVE ID : CVE-2023-1172</b>	<a href="https://plugins.trac.wordpress.org/changest?sf_email=&amp;sfph_mail=&amp;reponame=&amp;old=2876981%40bookly-responsive-appointment-booking-tool&amp;new=2876981%40bookly-responsive-appointment-booking-tool&amp;sf_email=&amp;sfph_mail=">https://plugins.trac.wordpress.org/changest?sf_email=&amp;sfph_mail=&amp;reponame=&amp;old=2876981%40bookly-responsive-appointment-booking-tool&amp;new=2876981%40bookly-responsive-appointment-booking-tool&amp;sf_email=&amp;sfph_mail=</a>	A-B00-BOOK-050423/198
--	-------------	-----	---	---	-----------------------

**Vendor: Broadcom**

**Product: tcpreplay**

Affected Version(s): 4.4.3

Reachable Assertion	16-Mar-2023	7.5	An issue found in TCPReplay tcprewrite v.4.4.3 allows a remote attacker to	<a href="https://github.com/appneta/tcpreplay/pull">https://github.com/appneta/tcpreplay/pull</a>	A-BRO-TCPR-050423/199
---------------------	-------------	-----	--	---	-----------------------

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
			cause a denial of service via the tcpedit_dlt_cleanup function at plugins/dlt_plugins.c. <b>CVE ID : CVE-2023-27783</b>	/781, <a href="https://github.com/ppneta/tcp-replay/issues/780">https://github.com/ppneta/tcp-replay/issues/780</a>	
NULL Pointer Dereference	16-Mar-2023	7.5	An issue found in TCPReplay v.4.4.3 allows a remote attacker to cause a denial of service via the read_hexstring function at the utils.c:309 endpoint. <b>CVE ID : CVE-2023-27784</b>	<a href="https://github.com/ppneta/tcp-replay/issues/787">https://github.com/ppneta/tcp-replay/issues/787</a>	A-BRO-TCPR-050423/200
NULL Pointer Dereference	16-Mar-2023	7.5	An issue found in TCPReplay TCPprep v.4.4.3 allows a remote attacker to cause a denial of service via the parse_endpoints function. <b>CVE ID : CVE-2023-27785</b>	<a href="https://github.com/ppneta/tcp-replay/issues/785">https://github.com/ppneta/tcp-replay/issues/785</a>	A-BRO-TCPR-050423/201
NULL Pointer Dereference	16-Mar-2023	7.5	An issue found in TCPprep v.4.4.3 allows a remote attacker to cause a denial of service via the macinstring function. <b>CVE ID : CVE-2023-27786</b>	<a href="https://github.com/ppneta/tcp-replay/pull/783">https://github.com/ppneta/tcp-replay/pull/783</a> , <a href="https://github.com/ppneta/tcp-replay/issues/782">https://github.com/ppneta/tcp-replay/issues/782</a>	A-BRO-TCPR-050423/202
NULL Pointer Dereference	16-Mar-2023	7.5	An issue found in TCPprep v.4.4.3 allows a remote attacker to cause a denial of service via the	<a href="https://github.com/ppneta/tcp-replay/issues/788">https://github.com/ppneta/tcp-replay/issues/788</a>	A-BRO-TCPR-050423/203

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
			parse_list function at the list.c:81 endpoint. <b>CVE ID : CVE-2023-27787</b>		
Reachable Assertion	16-Mar-2023	7.5	An issue found in TCPrewrite v.4.4.3 allows a remote attacker to cause a denial of service via the ports2PORT function at the portmap.c:69 endpoint. <b>CVE ID : CVE-2023-27788</b>	<a href="https://github.com/appneta/tcp-replay/issues/786">https://github.com/appneta/tcp-replay/issues/786</a>	A-BRO-TCPR-050423/204
Reachable Assertion	16-Mar-2023	7.5	An issue found in TCPprep v.4.4.3 allows a remote attacker to cause a denial of service via the cidr2cidr function at the cidr.c:178 endpoint. <b>CVE ID : CVE-2023-27789</b>	<a href="https://github.com/appneta/tcp-replay/pull/783">https://github.com/appneta/tcp-replay/pull/783</a> , <a href="https://github.com/appneta/tcp-replay/issues/784">https://github.com/appneta/tcp-replay/issues/784</a>	A-BRO-TCPR-050423/205
<b>Vendor: cal</b>					
<b>Product: cal.com</b>					
Affected Version(s): * Up to (excluding) 2.7.0					
N/A	27-Mar-2023	8.8	Improper Access Control in GitHub repository calcom/cal.com prior to 2.7. <b>CVE ID : CVE-2023-1647</b>	<a href="https://huntr.dev/bounties/d6de3d6e-9551-47d1-b28c-7e965c1b82b6">https://huntr.dev/bounties/d6de3d6e-9551-47d1-b28c-7e965c1b82b6</a> , <a href="https://github.com/calcom/cal.com/commit/c76e5f461">https://github.com/calcom/cal.com/commit/c76e5f461</a>	A-CAL-CAL.-050423/206

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
				01a826b2d e39123c22 f50c840dd dba0	
<b>Vendor: canteen_management_system_project</b>					
<b>Product: canteen_management_system</b>					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability was found in SourceCodester Canteen Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file changeUsername.php. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223304. <b>CVE ID : CVE-2023-1459</b>	N/A	A-CAN-CANT-050423/207
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability was found in SourceCodester Canteen Management System 1.0. It has been declared as critical. This vulnerability affects the function query of the file createCategories.php. The manipulation of the argument	N/A	A-CAN-CANT-050423/208

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
			categoriesStatus leads to sql injection. The attack can be initiated remotely. VDB-223306 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1461</b>		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Canteen Management System 1.0. This issue affects the function query of the file createuser.php. The manipulation of the argument uemail leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223337 was assigned to this vulnerability. <b>CVE ID : CVE-2023-1475</b>	N/A	A-CAN-CANT-050423/209
<b>Vendor: cerebrate-project</b>					
<b>Product: cerebrate</b>					
Affected Version(s): 1.13					
Improper Neutralization of Special Elements used in an SQL	27-Mar-2023	9.8	In Cerebrate 1.13, a blind SQL injection exists in the searchAll API endpoint. <b>CVE ID : CVE-2023-28883</b>	<a href="https://github.com/cerebrate-project/cerebrate/commit/5f1c99cd534442e">https://github.com/cerebrate-project/cerebrate/commit/5f1c99cd534442e</a>	A-CER-CERE-050423/210

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')				c40c21297 69608e3e6 1ff8be3	
<b>Vendor: churchcrm</b>					
<b>Product: churchcrm</b>					
Affected Version(s): 4.5.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	RESERVED churchcrm v4.5.3 was discovered to contain a SQL injection vulnerability via the Event parameter at /churchcrm/EventAttendance.php. <b>CVE ID : CVE-2023-24787</b>	N/A	A-CHU-CHUR-050423/211
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-2023	5.4	A cross-site scripting (XSS) vulnerability in the Edit Group function of ChurchCRM v4.5.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Edit Group Name text field. <b>CVE ID : CVE-2023-27059</b>	<a href="https://github.com/ChurchCRM/CRM/issues/6450">https://github.com/ChurchCRM/CRM/issues/6450</a>	A-CHU-CHUR-050423/212
<b>Vendor: cilium</b>					
<b>Product: cilium</b>					
Affected Version(s): * Up to (excluding) 1.11.15					
Incorrect Authorization	17-Mar-2023	7.3	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.11.15, 1.12.8, and 1.13.1,	N/A	A-CIL-CILI-050423/213

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
			<p>under specific conditions, Cilium may misattribute the source IP address of traffic to a cluster, identifying external traffic as coming from the host on which Cilium is running. As a consequence, network policies for that cluster might be bypassed, depending on the specific network policies enabled. This issue only manifests when Cilium is routing IPv6 traffic and NodePorts are used to route traffic to pods. IPv6 and endpoint routes are both disabled by default. The problem has been fixed and is available on versions 1.11.15, 1.12.8, and 1.13.1. As a workaround, disable IPv6 routing.</p> <p><b>CVE ID : CVE-2023-27594</b></p>		
Incorrect Default Permissions	17-Mar-2023	5.5	<p>Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.11.15, 1.12.8, and 1.13.1, an attacker with access to a Cilium agent pod can write to <code>/opt/cni/bin`</code></p>	N/A	A-CIL-CILI-050423/214

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
			<p>due to a `hostPath` mount of that directory in the agent pod. By replacing the CNI binary with their own malicious binary and waiting for the creation of a new pod on the node, the attacker can gain access to the underlying node. The issue has been fixed and the fix is available on versions 1.11.15, 1.12.8, and 1.13.1. Some workarounds are available. Kubernetes RBAC should be used to deny users and service accounts `exec` access to Cilium agent pods. In cases where a user requires `exec` access to Cilium agent pods, but should not have access to the underlying node, no workaround is possible.</p> <p><b>CVE ID : CVE-2023-27593</b></p>		
Affected Version(s): 1.13.0					
Improper Handling of Exceptional Conditions	17-Mar-2023	9.8	<p>Cilium is a networking, observability, and security solution with an eBPF-based dataplane. In version 1.13.0, when Cilium is started, there is a short period when</p>	N/A	A-CIL-CILI-050423/215

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
			<p>Cilium eBPF programs are not attached to the host. During this period, the host does not implement any of Cilium's featureset. This can cause disruption to newly established connections during this period due to the lack of Load Balancing, or can cause Network Policy bypass due to the lack of Network Policy enforcement during the window. This vulnerability impacts any Cilium-managed endpoints on the node (such as Kubernetes Pods), as well as the host network namespace (including Host Firewall). This vulnerability is fixed in Cilium 1.13.1 or later. Cilium releases 1.12.x, 1.11.x, and earlier are not affected. There are no known workarounds.</p> <p><b>CVE ID : CVE-2023-27595</b></p>		
Affected Version(s): From (including) 1.12.0 Up to (excluding) 1.12.8					
Incorrect Authorization	17-Mar-2023	7.3	<p>Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.11.15,</p>	N/A	A-CIL-CILI-050423/216

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
			<p>1.12.8, and 1.13.1, under specific conditions, Cilium may misattribute the source IP address of traffic to a cluster, identifying external traffic as coming from the host on which Cilium is running. As a consequence, network policies for that cluster might be bypassed, depending on the specific network policies enabled. This issue only manifests when Cilium is routing IPv6 traffic and NodePorts are used to route traffic to pods. IPv6 and endpoint routes are both disabled by default. The problem has been fixed and is available on versions 1.11.15, 1.12.8, and 1.13.1. As a workaround, disable IPv6 routing.</p> <p><b>CVE ID : CVE-2023-27594</b></p>		
Incorrect Default Permissions	17-Mar-2023	5.5	<p>Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.11.15, 1.12.8, and 1.13.1, an attacker with access to a Cilium agent pod can</p>	N/A	A-CIL-CILI-050423/217

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
			<p>write to `/opt/cni/bin` due to a `hostPath` mount of that directory in the agent pod. By replacing the CNI binary with their own malicious binary and waiting for the creation of a new pod on the node, the attacker can gain access to the underlying node. The issue has been fixed and the fix is available on versions 1.11.15, 1.12.8, and 1.13.1. Some workarounds are available. Kubernetes RBAC should be used to deny users and service accounts `exec` access to Cilium agent pods. In cases where a user requires `exec` access to Cilium agent pods, but should not have access to the underlying node, no workaround is possible.</p> <p><b>CVE ID : CVE-2023-27593</b></p>		
Affected Version(s): From (including) 1.13.0 Up to (excluding) 1.13.1					
Incorrect Authorization	17-Mar-2023	7.3	<p>Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.11.15, 1.12.8, and 1.13.1,</p>	N/A	A-CIL-CILI-050423/218

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
			<p>under specific conditions, Cilium may misattribute the source IP address of traffic to a cluster, identifying external traffic as coming from the host on which Cilium is running. As a consequence, network policies for that cluster might be bypassed, depending on the specific network policies enabled. This issue only manifests when Cilium is routing IPv6 traffic and NodePorts are used to route traffic to pods. IPv6 and endpoint routes are both disabled by default. The problem has been fixed and is available on versions 1.11.15, 1.12.8, and 1.13.1. As a workaround, disable IPv6 routing.</p> <p><b>CVE ID : CVE-2023-27594</b></p>		
Incorrect Default Permissions	17-Mar-2023	5.5	<p>Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.11.15, 1.12.8, and 1.13.1, an attacker with access to a Cilium agent pod can write to <code>/opt/cni/bin`</code></p>	N/A	A-CIL-CILI-050423/219

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
			<p>due to a `hostPath` mount of that directory in the agent pod. By replacing the CNI binary with their own malicious binary and waiting for the creation of a new pod on the node, the attacker can gain access to the underlying node. The issue has been fixed and the fix is available on versions 1.11.15, 1.12.8, and 1.13.1. Some workarounds are available. Kubernetes RBAC should be used to deny users and service accounts `exec` access to Cilium agent pods. In cases where a user requires `exec` access to Cilium agent pods, but should not have access to the underlying node, no workaround is possible.</p> <p><b>CVE ID : CVE-2023-27593</b></p>		

**Product: cilium-cli**

Affected Version(s): \* Up to (excluding) 0.13.2

Improper Handling of Insufficient Permissions or Privileges	22-Mar-2023	4.1	<p>`cilium-cli` is the command line interface to install, manage, and troubleshoot Kubernetes clusters running Cilium. Prior to version</p>	<p><a href="https://github.com/cilium/cilium-cli/security/advisories/GHSA-6f27-3p6c-">https://github.com/cilium/cilium-cli/security/advisories/GHSA-6f27-3p6c-</a></p>	A-CIL-CILI-050423/220
---	-------------	-----	---	--	-----------------------

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
			<p>0.13.2,`cilium-cli`, when used to configure cluster mesh functionality, can remove the enforcement of user permissions on the `etcd` store used to mirror local cluster information to remote clusters. Users who have set up cluster meshes using the Cilium Helm chart are not affected by this issue. Due to an incorrect mount point specification, the settings specified by the `initContainer` that configures `etcd` users and their permissions are overwritten when using `cilium-cli` to configure a cluster mesh. An attacker who has already gained access to a valid key and certificate for an `etcd` cluster compromised in this manner could then modify state in that `etcd` cluster. This issue is patched in `cilium-cli` 0.13.2. As a workaround, one may use Cilium's Helm charts to create their cluster.</p> <p><b>CVE ID : CVE-2023-28114</b></p>	<p>p5jc,  <a href="https://github.com/cilium/cilium">https://github.com/cilium/cilium</a>  -  cli/commit/  fb142702  5764e1eeb  c4a7710d9  02c4f22cae  2610</p>	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
<b>Vendor: Cisco</b>					
<b>Product: adaptive_security_appliance</b>					
Affected Version(s): 9.10.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/221

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/222

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.11					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/223

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/224

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/225

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.22					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/226

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.27					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/227

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.30					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/228

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.32					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/229

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.37					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/230

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.40					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/231

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.42					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/232

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.44					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/233

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/234

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/235

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/236

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.1.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/237

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/238

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.2.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/239

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.2.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/240

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.2.5					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/241

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.2.9					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/242

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/243

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.3.12					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/244

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.3.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/245

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.3.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/246

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.3.9					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/247

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/248

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/249

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthd-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthd-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/250

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.18					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/251

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/252

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.24					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/253

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/254

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.29					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/255

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.30					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/256

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.35					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/257

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.37					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/258

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/259

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/260

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/261

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/262

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/263

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.12					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/264

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/265

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.16					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/266

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.19					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/267

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/268

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.21					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/269

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/270

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/271

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/272

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.1.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/273

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.1.19					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/274

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.1.30					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/275

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.1.6					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/276

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/277

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.2.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/278

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.2.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/279

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.2.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/280

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.2.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/281

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/282

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.3.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/283

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.3.11					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/284

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.3.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/285

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.3.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/286

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.3.18					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/287

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.3.9					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/288

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.15.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/289

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.15.1.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/290

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.15.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/291

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.15.1.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/292

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.15.1.16					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/293

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.15.1.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/294

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.15.1.21					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/295

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.15.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/296

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.16.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/297

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.16.1.28					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/298

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.16.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/299

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.16.2.11					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/300

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.16.2.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/301

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.16.2.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/302

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.17.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/303

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/304

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.1.5					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/305

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/306

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/307

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.14					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/308

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/309

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/310

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.20					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/311

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.24					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/312

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/313

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.28					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/314

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.33					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/315

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.35					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/316

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.38					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/317

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.45					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/318

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/319

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/320

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3.11					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/321

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3.14					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/322

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3.16					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/323

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3.18					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/324

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3.21					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/325

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/326

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3.29					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/327

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/328

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/329

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/330

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.12					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/331

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/332

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/333

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.20					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/334

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.22					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/335

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.25					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/336

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/337

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.29					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/338

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/339

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.32					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/340

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.33					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/341

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.34					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/342

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.35					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/343

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.39					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/344

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.40					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/345

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.41					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/346

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.43					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/347

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.44					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/348

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.45					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/349

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/350

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/351

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/352

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/353

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.1.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/354

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.1.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/355

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.1.5					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/356

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/357

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/358

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.14					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/359

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.18					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/360

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.235					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/361

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.25					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/362

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.27					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/363

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.32					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/364

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.36					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/365

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.40					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/366

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.47					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/367

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.50					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/368

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.52					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/369

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.56					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/370

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.59					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/371

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.61					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/372

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.66					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/373

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.67					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/374

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.74					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/375

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.80					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/376

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.83					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/377

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.85					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/378

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
			<b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.9					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-ADAP-050423/379

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
			<b>CVE ID : CVE-2023-20081</b>		
<b>Product: aironet_access_point_software</b>					
Affected Version(s): * Up to (excluding) 17.9.0.135					
N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	A-CIS-AIRO-050423/380
<b>Product: catalyst_8000v_edge</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	A-CIS-CATA-050423/381

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
			<p>arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	rityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw	
<b>Product: dna_center</b>					
Affected Version(s): * Up to (excluding) 2.3.3.6					

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	23-Mar-2023	8.8	<p>A vulnerability in the management API of Cisco DNA Center could allow an authenticated, remote attacker to elevate privileges in the context of the web-based management interface on an affected device. This vulnerability is due to the unintended exposure of sensitive information. An attacker could exploit this vulnerability by inspecting the responses from the API. Under certain circumstances, a successful exploit could allow the attacker to access the API with the privileges of a higher-level user account. To successfully exploit this vulnerability, the attacker would need at least valid Observer credentials.</p> <p><b>CVE ID : CVE-2023-20055</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-dnac-privesc-QFXe74RS">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-dnac-privesc-QFXe74RS</a></p>	A-CIS-DNA_-050423/382
Affected Version(s): * Up to (excluding) 2.3.3.7					
Cleartext Storage of Sensitive Information	23-Mar-2023	6.5	<p>A vulnerability in the implementation of the Cisco Network Plug-and-Play (PnP) agent of Cisco DNA Center could allow an authenticated, remote attacker to view</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a></p>	A-CIS-DNA_-050423/383

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>sensitive information in clear text. The attacker must have valid low-privileged user credentials. This vulnerability is due to improper role-based access control (RBAC) with the integration of PnP. An attacker could exploit this vulnerability by authenticating to the device and sending a query to an internal API. A successful exploit could allow the attacker to view sensitive information in clear text, which could include configuration files.</p> <p><b>CVE ID : CVE-2023-20059</b></p>	dnac-infodisc-pe7zAbdR	
Affected Version(s): 2.3.4.0					
N/A	23-Mar-2023	8.8	<p>A vulnerability in the management API of Cisco DNA Center could allow an authenticated, remote attacker to elevate privileges in the context of the web-based management interface on an affected device. This vulnerability is due to the unintended exposure of sensitive information. An attacker could exploit this vulnerability by inspecting the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-privesc-QFXe74RS">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-privesc-QFXe74RS</a></p>	A-CIS-DNA_-050423/384

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
			<p>responses from the API. Under certain circumstances, a successful exploit could allow the attacker to access the API with the privileges of a higher-level user account. To successfully exploit this vulnerability, the attacker would need at least valid Observer credentials.</p> <p><b>CVE ID : CVE-2023-20055</b></p>		
Affected Version(s): From (including) 2.3.4.0 Up to (excluding) 2.3.5.0					
Cleartext Storage of Sensitive Information	23-Mar-2023	6.5	<p>A vulnerability in the implementation of the Cisco Network Plug-and-Play (PnP) agent of Cisco DNA Center could allow an authenticated, remote attacker to view sensitive information in clear text. The attacker must have valid low-privileged user credentials. This vulnerability is due to improper role-based access control (RBAC) with the integration of PnP. An attacker could exploit this vulnerability by authenticating to the device and sending a query to an internal API. A successful exploit could allow the attacker to view</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sadnac-infodisc-pe7zAbdR">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sadnac-infodisc-pe7zAbdR</a></p>	A-CIS-DNA-050423/385

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive information in clear text, which could include configuration files. <b>CVE ID : CVE-2023-20059</b>		
<b>Product: firepower_threat_defense</b>					
Affected Version(s): 9.10.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/386

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/387

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.11					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/388

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/389

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/390

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.22					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/391

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.27					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/392

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.30					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/393

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.32					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/394

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.37					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/395

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.40					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/396

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.42					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/397

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.44					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/398

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.10.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/399

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/400

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
			<p>attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
Affected Version(s): 9.12.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	A-CIS-FIRE-050423/401

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.1.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/402

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/403

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.2.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/404

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.2.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/405

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.2.5					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/406

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.2.9					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/407

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/408

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.3.12					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/409

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.3.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/410

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.3.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/411

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
			<p>attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
Affected Version(s): 9.12.3.9					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	A-CIS-FIRE-050423/412

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/413

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/414

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/415

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
Affected Version(s): 9.12.4.18					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	A-CIS-FIRE-050423/416

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/417

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.24					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/418

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/419

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.29					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/420

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.30					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/421

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.35					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/422

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.37					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/423

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/424

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/425

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.12.4.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/426

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/427

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/428

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.12					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/429

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/430

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.16					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/431

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.19					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/432

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/433

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.21					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/434

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.13.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/435

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/436

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/437

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.1.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/438

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.1.19					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/439

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.1.30					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/440

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.1.6					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/441

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/442

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.2.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/443

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.2.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/444

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.2.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/445

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.2.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/446

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/447

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.3.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/448

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.3.11					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/449

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.3.13					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/450

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.3.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/451

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.3.18					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/452

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.14.3.9					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/453

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.15.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/454

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.15.1.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/455

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.15.1.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/456

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
			<p>attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
Affected Version(s): 9.15.1.15					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	A-CIS-FIRE-050423/457

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.15.1.16					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/458

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.15.1.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/459

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.15.1.21					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/460

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.15.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/461

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.16.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/462

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
			<p>attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
Affected Version(s): 9.16.1.28					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	A-CIS-FIRE-050423/463

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.16.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/464

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.16.2.11					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/465

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.16.2.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/466

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.16.2.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/467

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.17.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/468

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/469

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.1.5					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/470

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.1.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/471

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/472

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.14					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/473

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.15					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/474

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/475

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.20					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/476

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.24					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/477

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/478

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.28					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/479

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.33					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/480

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.35					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/481

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.38					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/482

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.45					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/483

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.2.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/484

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/485

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
			<p>attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
Affected Version(s): 9.8.3.11					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	A-CIS-FIRE-050423/486

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3.14					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/487

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3.16					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/488

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3.18					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/489

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3.21					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/490

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/491

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3.29					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/492

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.3.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/493

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/494

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.10					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/495

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.12					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/496

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
			<p>attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
Affected Version(s): 9.8.4.15					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	A-CIS-FIRE-050423/497

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.17					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/498

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.20					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/499

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.22					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/500

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.25					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/501

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.26					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/502

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.29					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/503

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/504

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.32					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/505

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.33					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/506

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.34					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/507

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.35					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/508

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
			<p>attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
Affected Version(s): 9.8.4.39					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	A-CIS-FIRE-050423/509

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.40					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/510

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.41					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/511

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.43					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/512

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.44					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/513

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
			<p>attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
Affected Version(s): 9.8.4.45					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	A-CIS-FIRE-050423/514

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.7					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/515

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.8.4.8					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/516

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/517

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.1.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/518

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.1.3					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/519

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.1.4					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/520

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.1.5					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/521

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/522

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/523

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.14					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/524

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
			<p>attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
Affected Version(s): 9.9.2.18					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	A-CIS-FIRE-050423/525

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.235					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/526

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.25					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/527

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.27					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/528

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.32					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/529

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.36					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/530

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
			<p>attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
Affected Version(s): 9.9.2.40					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	A-CIS-FIRE-050423/531

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.47					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/532

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.50					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/533

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.52					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/534

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.56					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/535

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.59					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/536

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.61					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/537

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.66					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/538

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.67					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/539

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.74					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/540

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.80					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/541

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.83					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/542

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.85					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/543

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): 9.9.2.9					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	A-CIS-FIRE-050423/544

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: wireless_lan_controller_software</b>					
Affected Version(s): * Up to (excluding) 8.10.183.0					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	A-CIS-WIRE-050423/545
<b>Vendor: Ckeditor</b>					
<b>Product: ckeditor</b>					

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): From (including) 4.0 Up to (excluding) 4.21.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. A cross-site scripting vulnerability has been discovered affecting Iframe Dialog and Media Embed packages. The vulnerability may trigger a JavaScript code after fulfilling special conditions: using one of the affected packages on a web page with missing proper Content Security Policy configuration; initializing the editor on an element and using an element other than ` <textarea>` as a base; and destroying the editor instance. This vulnerability might affect a small percentage of integrators that depend on dynamic editor initialization/destroy mechanism. A fix is available in CKEditor4 version 4.21.0. In some rare cases, a security fix may be considered a breaking change. Starting from version 4.21.0, the Iframe Dialog plugin applies the `sandbox`&lt;/td&gt; &lt;td&gt;&lt;a href="https://github.com/ckeditor/ckeditor4/security/advisories/GHSA-vh5c-xwqv-cv9g"&gt;https://github.com/ckeditor/ckeditor4/security/advisories/GHSA-vh5c-xwqv-cv9g&lt;/a&gt;&lt;/td&gt; &lt;td&gt;A-CKE-CKED-050423/546&lt;/td&gt; &lt;/tr&gt; &lt;/tbody&gt; &lt;/table&gt; &lt;/div&gt; &lt;div data-bbox="81 925 917 942" data-label="Table"&gt; &lt;table border="1"&gt; &lt;tr&gt; &lt;td&gt;CVSS Scoring Scale&lt;/td&gt; &lt;td&gt;0-1&lt;/td&gt; &lt;td&gt;1-2&lt;/td&gt; &lt;td&gt;2-3&lt;/td&gt; &lt;td&gt;3-4&lt;/td&gt; &lt;td&gt;4-5&lt;/td&gt; &lt;td&gt;5-6&lt;/td&gt; &lt;td&gt;6-7&lt;/td&gt; &lt;td&gt;7-8&lt;/td&gt; &lt;td&gt;8-9&lt;/td&gt; &lt;td&gt;9-10&lt;/td&gt; &lt;/tr&gt; &lt;/table&gt; &lt;/div&gt; &lt;div data-bbox="437 942 559 956" data-label="Page-Footer"&gt; &lt;p&gt;Page 427 of 2442&lt;/p&gt; &lt;/div&gt;</textarea>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>attribute by default, which restricts JavaScript code execution in the iframe element. To change this behavior, configure the `config.iframe_attributes` option. Also starting from version 4.21.0, the Media Embed plugin regenerates the entire content of the embed widget by default. To change this behavior, configure the `config.embed_keepOriginalContent` option. Those who choose to enable either of the more permissive options or who cannot upgrade to a patched version should properly configure Content Security Policy to avoid any potential security issues that may arise from embedding iframe elements on their web page.</p> <p><b>CVE ID : CVE-2023-28439</b></p>		
<b>Vendor: cloudflare</b>					
<b>Product: cloudflared</b>					
Affected Version(s): * Up to (excluding) 2023.3.1					
Improper Link Resolution Before File	21-Mar-2023	7.8	A vulnerability has been discovered in cloudflared's installer (<= 2023.3.0) for	<a href="https://github.com/cloudflare/cloudflared">https://github.com/cloudflare/cloudflared/s</a>	A-CLO-CLOU-050423/547

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access ('Link Following')			Windows 32-bits devices that allows a local attacker with no administrative permissions to escalate their privileges on the affected device. This vulnerability exists because the MSI installer used by cloudflared relied on a world-writable directory. An attacker with local access to the device (without Administrator rights) can use symbolic links to trick the MSI installer into deleting files in locations that the attacker would otherwise have no access to. By creating a symlink from the world-writable directory to the target file, the attacker can manipulate the MSI installer's repair functionality to delete the target file during the repair process. Exploitation of this vulnerability could allow an attacker to delete important system files or replace them with malicious files, potentially leading to the affected device being compromised. The cloudflared client	security/advisories/GHSA-7mjb-x3jf-545x	

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
			itself is not affected by this vulnerability, only the installer for 32-bit Windows devices. <b>CVE ID : CVE-2023-1314</b>		
<b>Vendor: Cminds</b>					
<b>Product: cm_answers</b>					
Affected Version(s): * Up to (including) 3.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in CreativeMindsSolutions CM Answers plugin <= 3.1.9 versions. <b>CVE ID : CVE-2023-25992</b>	N/A	A-CMI-CM_A-050423/548
<b>Vendor: codemenschen</b>					
<b>Product: gift_vouchers</b>					
Affected Version(s): * Up to (including) 4.3.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	The Gift Cards (Gift Vouchers and Packages) WordPress Plugin, version <= 4.3.1, is affected by an unauthenticated SQL injection vulnerability in the template parameter in the wpgv_doajax_voucher_pdf_save_func action. <b>CVE ID : CVE-2023-28662</b>	N/A	A-COD-GIFT-050423/549
<b>Vendor: coder</b>					
<b>Product: code-server</b>					
Affected Version(s): * Up to (excluding) 4.10.1					

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
Origin Validation Error	23-Mar-2023	9.3	<p>Versions of the package code-server before 4.10.1 are vulnerable to Missing Origin Validation in WebSockets handshakes. Exploiting this vulnerability can allow an adversary in specific scenarios to access data from and connect to the code-server instance.</p> <p><b>CVE ID : CVE-2023-26114</b></p>	<p><a href="https://github.com/code-server/code-server/commit/d477972c68fc8c8e8d610aa7287db87ba90e55c7">https://github.com/code-server/code-server/commit/d477972c68fc8c8e8d610aa7287db87ba90e55c7</a>,  <a href="https://security.snyk.io/vuln/SNYK-JS-CODESERV-ER-3368148">https://security.snyk.io/vuln/SNYK-JS-CODESERV-ER-3368148</a></p>	A-COD-CODE-050423/550
<b>Vendor: collection.js_project</b>					
<b>Product: collection.js</b>					
Affected Version(s): * Up to (excluding) 6.8.1					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	18-Mar-2023	7.5	<p>Versions of the package collection.js before 6.8.1 are vulnerable to Prototype Pollution via the extend function in Collection.js/dist/node/iterators/extend.js.</p> <p><b>CVE ID : CVE-2023-26113</b></p>	<p><a href="https://github.com/kobeazza/Collection/commit/d3d937645f62f37d3115d6aa90bb510fd856e6a2">https://github.com/kobeazza/Collection/commit/d3d937645f62f37d3115d6aa90bb510fd856e6a2</a>,  <a href="https://github.com/kobeazza/Collection/issues/27">https://github.com/kobeazza/Collection/issues/27</a>,  <a href="https://github.com/kobeazza/Collection/releases/tag/v6.8.1">https://github.com/kobeazza/Collection/releases/tag/v6.8.1</a></p>	A-COL-COLL-050423/551
<b>Vendor: corebos</b>					
<b>Product: corebos</b>					

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): * Up to (excluding) 8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-2023	5.4	Cross-site Scripting (XSS) - Generic in GitHub repository tsolucio/corebos prior to 8.0. <b>CVE ID : CVE-2023-1527</b>	<a href="https://github.com/tsolucio/corebos/commit/aaaca69185bce2be6a82956c69541938dc871268">https://github.com/tsolucio/corebos/commit/aaaca69185bce2be6a82956c69541938dc871268</a> , <a href="https://huntr.dev/bounties/f0272a31-9944-4545-8428-a26154d20348">https://huntr.dev/bounties/f0272a31-9944-4545-8428-a26154d20348</a>	A-COR-CORE-050423/552
<b>Vendor: couchbase</b>					
<b>Product: couchbase_server</b>					
Affected Version(s): From (including) 6.6.0 Up to (excluding) 7.1.4					
Missing Authentication for Critical Function	23-Mar-2023	5.3	In Couchbase Server 5 through 7 before 7.1.4, the nsstats endpoint is accessible without authentication. <b>CVE ID : CVE-2023-28470</b>	<a href="https://www.couchbase.com/alerts/">https://www.couchbase.com/alerts/</a> , <a href="https://forums.couchbase.com/tags/security">https://forums.couchbase.com/tags/security</a>	A-COU-COUC-050423/553
<b>Vendor: courtbouillon</b>					
<b>Product: cairosvg</b>					
Affected Version(s): * Up to (excluding) 2.7.0					
Server-Side Request Forgery (SSRF)	20-Mar-2023	7.1	CairoSVG is an SVG converter based on Cairo, a 2D graphics library. Prior to version 2.7.0, Cairo can send requests to external hosts when processing SVG files. A	<a href="https://github.com/Kozea/CairoSVG/security/advisories/GHSA-rwmf-w63j-p7gv">https://github.com/Kozea/CairoSVG/security/advisories/GHSA-rwmf-w63j-p7gv</a> ,	A-COU-CAIR-050423/554

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
			malicious actor could send a specially crafted SVG file that allows them to perform a server-side request forgery or denial of service. Version 2.7.0 disables CairoSVG's ability to access other files online by default. <b>CVE ID : CVE-2023-27586</b>	<a href="https://github.com/Kozea/CairoSVG/commit/12d31c653c0254fa9d9853f66b04ea46e7397255">https://github.com/Kozea/CairoSVG/commit/12d31c653c0254fa9d9853f66b04ea46e7397255</a> , <a href="https://github.com/Kozea/CairoSVG/commit/33007d4af9195e2fb2ff9af064c4c2d8e4b2b53">https://github.com/Kozea/CairoSVG/commit/33007d4af9195e2fb2ff9af064c4c2d8e4b2b53</a>	

**Vendor: crmeb**

**Product: crmeb\_java**

Affected Version(s): \* Up to (including) 1.3.4

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	A vulnerability was found in Zhong Bang CRMEB Java up to 1.3.4. It has been declared as critical. This vulnerability affects the function getAdminList of the file /api/admin/store/product/list. The manipulation of the argument cateId leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-223738 is the identifier assigned to this vulnerability.	N/A	A-CRM-CRME-050423/555
--	-------------	-----	--	-----	-----------------------

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
			<b>CVE ID : CVE-2023-1608</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	5.4	A vulnerability was found in Zhong Bang CRMEB Java up to 1.3.4. It has been rated as problematic. This issue affects the function save of the file /api/admin/store/product/save. The manipulation 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-223739. <b>CVE ID : CVE-2023-1609</b>	N/A	A-CRM-CRME-050423/556
<b>Vendor: custom_content_shortcode_project</b>					
<b>Product: custom_content_shortcode</b>					
Affected Version(s): * Up to (including) 4.0.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Mar-2023	8.8	The Custom Content Shortcode WordPress plugin through 4.0.2 does not validate one of its shortcode attribute, which could allow users with a contributor role and above to include arbitrary files via a traversal attack. This could also allow them to read non PHP files and retrieve their content. RCE could	N/A	A-CUS-CUST-050423/557

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
			also be achieved if the attacker manage to upload a malicious image containing PHP code, and then include it via the affected attribute, on a default WP install, authors could easily achieve that given that they have the upload_file capability. <b>CVE ID : CVE-2023-0340</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Custom Content Shortcode WordPress plugin through 4.0.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks <b>CVE ID : CVE-2023-0273</b>	N/A	A-CUS-CUST-050423/558
<b>Vendor: databasir</b>					
<b>Product: databasir</b>					
Affected Version(s): 1.0.7					
Improper Neutralization of Special Elements used in an Expression	28-Mar-2023	9.8	Databasir v1.0.7 was discovered to contain a remote code execution (RCE) vulnerability via the	N/A	A-DAT-DATA-050423/559

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
Language Statement ('Expression Language Injection')			mockDataScript parameter. <b>CVE ID : CVE-2023-27821</b>		
<b>Vendor: dataease</b>					
<b>Product: dataease</b>					
Affected Version(s): * Up to (excluding) 1.18.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Mar-2023	9.8	Dataease is an open source data visualization and analysis tool. The blacklist for SQL injection protection is missing entries. This vulnerability has been fixed in version 1.18.5. There are no known workarounds. <b>CVE ID : CVE-2023-28437</b>	<a href="https://github.com/dataease/dataease/issues/4795">https://github.com/dataease/dataease/issues/4795</a> , <a href="https://github.com/dataease/dataease/security/advisories/GHSA-7j7j-9rw6-3r56">https://github.com/dataease/dataease/security/advisories/GHSA-7j7j-9rw6-3r56</a>	A-DAT-DATA-050423/560
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Mar-2023	6.1	Dataease is an open source data visualization and analysis tool. The permissions for the file upload interface is not checked so users who are not logged in can upload directly to the background. The file type also goes unchecked, users could upload any type of file. These vulnerabilities has been fixed in version 1.18.5. <b>CVE ID : CVE-2023-28435</b>	<a href="https://github.com/dataease/dataease/security/advisories/GHSA-625h-q3g9-rffc">https://github.com/dataease/dataease/security/advisories/GHSA-625h-q3g9-rffc</a>	A-DAT-DATA-050423/561
<b>Vendor: datagear</b>					

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
<b>Product: datagear</b>					
Affected Version(s): * Up to (excluding) 1.12.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A vulnerability has been found in DataGear up to 1.11.1 and classified as problematic. This vulnerability affects unknown code of the component Plugin Handler. The manipulation leads to cross site scripting. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. Upgrading to version 1.12.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-223564.  <b>CVE ID : CVE-2023-1572</b>	<a href="https://github.com/datageartech/datagear/releases/tag/v1.12.0">https://github.com/datageartech/datagear/releases/tag/v1.12.0</a>	A-DAT-DATA-050423/562
Affected Version(s): * Up to (including) 1.11.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	A vulnerability was found in DataGear up to 1.11.1 and classified as problematic. This issue affects some unknown processing of the component Graph Dataset Handler. The manipulation leads to cross site scripting. The attack may be	N/A	A-DAT-DATA-050423/563

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.12.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-223565 was assigned to this vulnerability.</p> <p><b>CVE ID : CVE-2023-1573</b></p>		
Affected Version(s): * Up to (including) 4.5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	<p>A vulnerability, which was classified as critical, was found in DataGear up to 4.5.0. This affects an unknown part of the file /analysisProject/pagingQueryData. The manipulation of the argument queryOrder leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.5.1 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-223563.</p>	N/A	A-DAT-DATA-050423/564

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
			<b>CVE ID : CVE-2023-1571</b>		
<b>Vendor: Dedecms</b>					
<b>Product: dedecms</b>					
Affected Version(s): * Up to (including) 5.7.106					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Mar-2023	7.2	SQL injection vulnerability found in DedeCMS v.5.7.106 allows a remote attacker to execute arbitrary code via the rank_* parameter in the /dede/group_store.php endpoint. <b>CVE ID : CVE-2023-27707</b>	N/A	A-DED-DEDE-050423/565
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Mar-2023	7.2	SQL injection vulnerability found in DedeCMS v.5.7.106 allows a remote attacker to execute arbitrary code via the rank_* parameter in the /dedestory_catalog.php endpoint. <b>CVE ID : CVE-2023-27709</b>	N/A	A-DED-DEDE-050423/566
<b>Vendor: deltaww</b>					
<b>Product: infrasuite_device_master</b>					
Affected Version(s): * Up to (excluding) 1.0.5					
Deserialization of Untrusted Data	27-Mar-2023	9.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contain a vulnerability in which the Device-status service listens on port 10100/ UDP by	N/A	A-DEL-INFR-050423/567

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
			default. The service accepts the unverified UDP packets and deserializes the content, which could allow an unauthenticated attacker to remotely execute arbitrary code. <b>CVE ID : CVE-2023-1133</b>		
Missing Authentication for Critical Function	27-Mar-2023	9.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contain a vulnerability that could allow an attacker to achieve unauthenticated remote code execution in the context of an administrator. <b>CVE ID : CVE-2023-1140</b>	N/A	A-DEL-INFR-050423/568
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Mar-2023	9.8	In Delta Electronics InfraSuite Device Master versions prior to 1.0.5, an attacker could use URL decoding to retrieve system files, credentials, and bypass authentication resulting in privilege escalation. <b>CVE ID : CVE-2023-1142</b>	N/A	A-DEL-INFR-050423/569
Improper Limitation of a Pathname	27-Mar-2023	8.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 are affected by	N/A	A-DEL-INFR-050423/570

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			a path traversal vulnerability, which could allow an attacker to read local files, disclose plaintext credentials, and escalate privileges. <b>CVE ID : CVE-2023-1134</b>		
Insufficiently Protected Credentials	27-Mar-2023	8.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contain a vulnerability in which a low-level user could extract files and plaintext credentials of administrator users, resulting in privilege escalation. <b>CVE ID : CVE-2023-1137</b>	N/A	A-DEL-INFR-050423/571
Deserialization of Untrusted Data	27-Mar-2023	8.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 are affected by a deserialization vulnerability targeting the Device-gateway service, which could allow deserialization of requests prior to authentication, resulting in remote code execution. <b>CVE ID : CVE-2023-1139</b>	N/A	A-DEL-INFR-050423/572
Improper Neutralization of Special Elements	27-Mar-2023	8.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contain a command injection	N/A	A-DEL-INFR-050423/573

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			vulnerability that could allow an attacker to inject arbitrary commands, which could result in remote code execution. <b>CVE ID : CVE-2023-1141</b>		
N/A	27-Mar-2023	8.8	In Delta Electronics InfraSuite Device Master versions prior to 1.0.5, an attacker could use Lua scripts, which could allow an attacker to remotely execute arbitrary code. <b>CVE ID : CVE-2023-1143</b>	N/A	A-DEL-INFR-050423/574
Incorrect Authorization	27-Mar-2023	8.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contains an improper access control vulnerability in which an attacker can use the Device-Gateway service and bypass authorization, which could result in privilege escalation. <b>CVE ID : CVE-2023-1144</b>	N/A	A-DEL-INFR-050423/575
Incorrect Permission Assignment for Critical Resource	27-Mar-2023	7.8	In Delta Electronics InfraSuite Device Master versions prior to 1.0.5, an attacker could set incorrect directory permissions, which could result in	N/A	A-DEL-INFR-050423/576

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
			local privilege escalation. <b>CVE ID : CVE-2023-1135</b>		
Deserializa tion of Untrusted Data	27-Mar-2023	7.8	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 are affected by a deserialization vulnerability targeting the Device-DataCollect service, which could allow deserialization of requests prior to authentication, resulting in remote code execution. <b>CVE ID : CVE-2023-1145</b>	N/A	A-DEL-INFR- 050423/577
Incorrect Authorizati on	27-Mar-2023	7.5	In Delta Electronics InfraSuite Device Master versions prior to 1.0.5, an unauthenticated attacker could generate a valid token, which would lead to authentication bypass. <b>CVE ID : CVE-2023-1136</b>	N/A	A-DEL-INFR- 050423/578
N/A	27-Mar-2023	7.5	Delta Electronics InfraSuite Device Master versions prior to 1.0.5 contain an improper access control vulnerability, which could allow an attacker to retrieve Gateway configuration files to obtain plaintext credentials.	N/A	A-DEL-INFR- 050423/579

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-1138</b>		
<b>Vendor: deno</b>					
<b>Product: deno</b>					
Affected Version(s): * Up to (excluding) 1.31.2					
Improper Neutralization of Escape, Meta, or Control Sequences	24-Mar-2023	8.8	<p>Deno is a simple, modern and secure runtime for JavaScript and TypeScript that uses V8 and is built in Rust. Arbitrary program names without any ANSI filtering allows any malicious program to clear the first 2 lines of a `op_spawn_child` or `op_kill` prompt and replace it with any desired text. This works with any command on the respective platform, giving the program the full ability to choose what program they wanted to run. This problem can not be exploited on systems that do not attach an interactive prompt (for example headless servers). This issue has been patched in version 1.31.2.</p> <p><b>CVE ID : CVE-2023-28446</b></p>	<p><a href="https://github.com/denoland/deno/blob/7d13d65468c37022f003bb680dfbdd07ea72173/runtime/js/40_process.js#L175">https://github.com/denoland/deno/blob/7d13d65468c37022f003bb680dfbdd07ea72173/runtime/js/40_process.js#L175</a>,  <a href="https://github.com/denoland/deno/releases/tag/v1.31.2">https://github.com/denoland/deno/releases/tag/v1.31.2</a>,  <a href="https://github.com/denoland/deno/security/advisories/GHSA-vq67-rp93-65qf">https://github.com/denoland/deno/security/advisories/GHSA-vq67-rp93-65qf</a></p>	A-DEN-DENO-050423/580
Affected Version(s): 1.32.0					

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
Out-of-bounds Read	24-Mar-2023	9.8	<p>Deno is a runtime for JavaScript and TypeScript that uses V8 and is built in Rust. Resizable ArrayBuffers passed to asynchronous functions that are shrunk during the asynchronous operation could result in an out-of-bound read/write. It is unlikely that this has been exploited in the wild, as the only version affected is Deno 1.32.0. Deno Deploy users are not affected. The problem has been resolved by disabling resizable ArrayBuffers temporarily in Deno 1.32.1. Deno 1.32.2 will re-enable resizable ArrayBuffers with a proper fix. As a workaround, run with `--v8-flags=--no-harmony-rab-gsab` to disable resizable ArrayBuffers.</p> <p><b>CVE ID : CVE-2023-28445</b></p>	<p><a href="https://github.com/denoland/deno/pull/18395">https://github.com/denoland/deno/pull/18395</a>,  <a href="https://github.com/denoland/deno/releases/tag/v1.32.1">https://github.com/denoland/deno/releases/tag/v1.32.1</a>,  <a href="https://github.com/denoland/deno/security/advisories/GHSA-c25x-cm9x-qgqx">https://github.com/denoland/deno/security/advisories/GHSA-c25x-cm9x-qgqx</a></p>	A-DEN-DENO-050423/581
<b>Product: deno_runtime</b>					
Affected Version(s): 0.102.0					
Out-of-bounds Read	24-Mar-2023	9.8	<p>Deno is a runtime for JavaScript and TypeScript that uses V8 and is built in Rust. Resizable ArrayBuffers passed</p>	<p><a href="https://github.com/denoland/deno/pull/18395">https://github.com/denoland/deno/pull/18395</a>,  <a href="https://github.com/denoland/deno/pull/18395">https://github.com/denoland/deno/pull/18395</a></p>	A-DEN-DENO-050423/582

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>to asynchronous functions that are shrunk during the asynchronous operation could result in an out-of-bound read/write. It is unlikely that this has been exploited in the wild, as the only version affected is Deno 1.32.0. Deno Deploy users are not affected. The problem has been resolved by disabling resizable ArrayBuffers temporarily in Deno 1.32.1. Deno 1.32.2 will re-enable resizable ArrayBuffers with a proper fix. As a workaround, run with `--v8-flags=--no-harmony-rab-gsab` to disable resizable ArrayBuffers.</p> <p><b>CVE ID : CVE-2023-28445</b></p>	<p>hub.com/denoland/deno/releases/tag/v1.32.1,  <a href="https://github.com/denoland/deno/security/advisories/GHSA-c25x-cm9x-qqgx">https://github.com/denoland/deno/security/advisories/GHSA-c25x-cm9x-qqgx</a></p>	

**Product: serde\_v8**

Affected Version(s): 0.87.0

Out-of-bounds Read	24-Mar-2023	9.8	<p>Deno is a runtime for JavaScript and TypeScript that uses V8 and is built in Rust. Resizable ArrayBuffers passed to asynchronous functions that are shrunk during the asynchronous operation could result in an out-of-bound</p>	<p><a href="https://github.com/denoland/deno/pull/18395">https://github.com/denoland/deno/pull/18395</a>,  <a href="https://github.com/denoland/deno/releases/tag/v1.32.1">https://github.com/denoland/deno/releases/tag/v1.32.1</a>,  <a href="https://github.com/denoland/deno/releases/tag/v1.32.1">https://github.com/denoland/deno/releases/tag/v1.32.1</a></p>	A-DEN-SERD-050423/583
--------------------	-------------	-----	---	--	-----------------------

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
			<p>read/write. It is unlikely that this has been exploited in the wild, as the only version affected is Deno 1.32.0. Deno Deploy users are not affected. The problem has been resolved by disabling resizable ArrayBuffers temporarily in Deno 1.32.1. Deno 1.32.2 will re-enable resizable ArrayBuffers with a proper fix. As a workaround, run with `--v8-flags=--no-harmony-rab-gsab` to disable resizable ArrayBuffers.</p> <p><b>CVE ID : CVE-2023-28445</b></p>	<p>hub.com/denoland/deno/security/advisories/GHSA-c25x-cm9x-qqgx</p>	

**Vendor: Dino**

**Product: dino**

Affected Version(s): \* Up to (excluding) 0.2.3

<p>Authorization Bypass Through User-Controlled Key</p>	<p>24-Mar-2023</p>	<p>7.1</p>	<p>Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information.</p> <p><b>CVE ID : CVE-2023-28686</b></p>	<p><a href="https://deno.im/security/cve-2023-28686/">https://deno.im/security/cve-2023-28686/</a></p>	<p>A-DIN-DINO-050423/584</p>
---	--------------------	------------	---	--	------------------------------

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): From (including) 0.3.0 Up to (excluding) 0.3.2					
Authorization Bypass Through User-Controlled Key	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information.  <b>CVE ID : CVE-2023-28686</b>	<a href="https://dino.im/security/cve-2023-28686/">https://dino.im/security/cve-2023-28686/</a>	A-DIN-DINO-050423/585
Affected Version(s): From (including) 0.4.0 Up to (excluding) 0.4.2					
Authorization Bypass Through User-Controlled Key	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information.  <b>CVE ID : CVE-2023-28686</b>	<a href="https://dino.im/security/cve-2023-28686/">https://dino.im/security/cve-2023-28686/</a>	A-DIN-DINO-050423/586
<b>Vendor: discourse</b>					
<b>Product: discourse</b>					
Affected Version(s): 1.1.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the	<a href="https://github.com/discourse/discourse/pull">https://github.com/discourse/discourse/pull</a>	A-DIS-DISC-050423/587

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
			<p>`stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>	<p>/20004,  <a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164</a>,  <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and</p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0">https://github.com/discourse/discourse/commit/f31f0</a></p>	A-DIS-DISC-050423/588

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
			<p>versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>	<p>b70f82c43d93220ce6fc0d4f57440452f37,  <a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a></p>	
Affected Version(s): 1.2.0					
N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-</p>	<p><a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a>,  <a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a></p>	A-DIS-DISC-050423/589

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
			<p>passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>	<a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164</a> ,	
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed`</p>	<a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f5744">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f5744</a>	A-DIS-DISC-050423/590

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
			<p>branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>	0452f37, <a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a>	
Affected Version(s): 3.0.0					
N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a</p>	<a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a> , <a href="https://github.com/discourse/discourse/commit/105f">https://github.com/discourse/discourse/commit/105f</a>	A-DIS-DISC-050423/591

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
			<p>count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>	<p>ee978d73b0ec23ff814a09d1c0c9ace95164,  <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a</p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a>,  <a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a></p>	A-DIS-DISC-050423/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>	<p>scourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</p>	
Affected Version(s): * Up to (excluding) 3.0.0					
N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in</p>	<p><a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a>,  <a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9</a></p>	A-DIS-DISC-050423/593

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
			<p>a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>	<p>ace95164,  <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	
Affected Version(s): * Up to (excluding) 3.0.1					
<p>Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')</p>	17-Mar-2023	5.4	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, a maliciously crafted URL can be included in a user's full name field to to carry out cross-site scripting</p>	<p><a href="https://github.com/discourse/discourse/commit/1a5a6f66cb821ed29a737311d6fdc2eba5adc915">https://github.com/discourse/discourse/commit/1a5a6f66cb821ed29a737311d6fdc2eba5adc915</a>,  <a href="https://github.com/discourse/discourse/sec">https://github.com/discourse/discourse/sec</a></p>	A-DIS-DISC-050423/594

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
			<p>attacks on sites with a disabled or overly permissive CSP (Content Security Policy). Discourse's default CSP prevents this vulnerability. The vulnerability is patched in version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches. As a workaround, enable and/or restore your site's CSP to the default one provided with Discourse.</p> <p><b>CVE ID : CVE-2023-25172</b></p>	<p>urity/advisories/GHSA-7pm2-prxw-wrvp, <a href="https://github.com/discourse/discourse/pull/20008">https://github.com/discourse/discourse/pull/20008</a></p>	
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the</p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a>, <a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a></p>	A-DIS-DISC-050423/595

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
			<p>user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>		
Affected Version(s): * Up to (excluding) 3.1.0					
Server-Side Request Forgery (SSRF)	17-Mar-2023	8.1	<p>Discourse is an open-source discussion platform. Prior to version 3.1.0.beta3 of the `beta` and `tests-passed` branches, some user provided URLs were being passed to FastImage without SSRF protection. Insufficient protections could enable attackers to trigger outbound network connections from the Discourse server to private IP addresses. This affects any site running the `tests-passed` or `beta` branches versions 3.1.0.beta2 and prior. This issue is patched</p>	<p><a href="https://github.com/discourse/discourse/pull/20710">https://github.com/discourse/discourse/pull/20710</a>,  <a href="https://github.com/discourse/discourse/security/advisories/GHSA-9897-x229-55gh">https://github.com/discourse/discourse/security/advisories/GHSA-9897-x229-55gh</a>,  <a href="https://github.com/discourse/discourse/commit/39c2f63b35d90ebaf67b9604cf1d424e5984203c">https://github.com/discourse/discourse/commit/39c2f63b35d90ebaf67b9604cf1d424e5984203c</a></p>	A-DIS-DISC-050423/596

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
			in version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds. <b>CVE ID : CVE-2023-28112</b>		
Server-Side Request Forgery (SSRF)	17-Mar-2023	7.5	Discourse is an open-source discussion platform. Prior to version 3.1.0.beta3 of the `beta` and `tests-passed` branches, attackers are able to bypass Discourse's server-side request forgery (SSRF) protection for private IPv4 addresses by using a IPv4-mapped IPv6 address. The issue is patched in the latest beta and tests-passed version of Discourse. version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds. <b>CVE ID : CVE-2023-28111</b>	<a href="https://github.com/discourse/discourse/pull/20710">https://github.com/discourse/discourse/pull/20710</a> , <a href="https://github.com/discourse/discourse/security/advisories/GHSA-26h3-8ww8-v5fc">https://github.com/discourse/discourse/security/advisories/GHSA-26h3-8ww8-v5fc</a> , <a href="https://github.com/discourse/discourse/commit/fd16eade7fcc6bba4b71e71106a2eb13cdfdae4a">https://github.com/discourse/discourse/commit/fd16eade7fcc6bba4b71e71106a2eb13cdfdae4a</a>	A-DIS-DISC-050423/597
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Mar-2023	5.4	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, a maliciously crafted URL can be included	<a href="https://github.com/discourse/discourse/commit/1a5a6f66cb821ed29a737311d6fdc2eba5adc915">https://github.com/discourse/discourse/commit/1a5a6f66cb821ed29a737311d6fdc2eba5adc915</a> , <a href="https://github.com/discourse/discourse/commit/1a5a6f66cb821ed29a737311d6fdc2eba5adc915">https://github.com/discourse/discourse/commit/1a5a6f66cb821ed29a737311d6fdc2eba5adc915</a>	A-DIS-DISC-050423/598

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>in a user's full name field to to carry out cross-site scripting attacks on sites with a disabled or overly permissive CSP (Content Security Policy). Discourse's default CSP prevents this vulnerability. The vulnerability is patched in version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches. As a workaround, enable and/or restore your site's CSP to the default one provided with Discourse.</p> <p><b>CVE ID : CVE-2023-25172</b></p>	<p>hub.com/discourse/discourse/security/advisories/GHSA-7pm2-prxw-wrvp, <a href="https://github.com/discourse/discourse/pull/20008">https://github.com/discourse/discourse/pull/20008</a></p>	
Allocation of Resources Without Limits or Throttling	17-Mar-2023	4.9	<p>Discourse is an open-source discussion platform. Prior to version 3.0.2 of the `stable` branch and version 3.1.0.beta3 of the `beta` and `tests-passed` branches, a user logged as an administrator can request backups multiple times, which will eat up all the connections to the DB. If this is done on a site using multisite, then it can affect the whole cluster. The vulnerability is</p>	<p><a href="https://github.com/discourse/discourse/commit/78a3efa7104eed6dd3ed7a06a71e2705337d9e61">https://github.com/discourse/discourse/commit/78a3efa7104eed6dd3ed7a06a71e2705337d9e61</a>, <a href="https://github.com/discourse/discourse/pull/20700">https://github.com/discourse/discourse/pull/20700</a>, <a href="https://github.com/discourse/discourse/security/advisories/GHSA-050423/599">https://github.com/discourse/discourse/security/advisories/GHSA-050423/599</a></p>	A-DIS-DISC-050423/599

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
			<p>patched in version 3.0.2 of the `stable` branch and version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds.</p> <p><b>CVE ID : CVE-2023-28107</b></p>	<p>ories/GHSA-cp7c-fm4c-6xxx</p>	
Affected Version(s): * Up to (including) 3.0.1					
Allocation of Resources Without Limits or Throttling	17-Mar-2023	4.9	<p>Discourse is an open-source discussion platform. Prior to version 3.0.2 of the `stable` branch and version 3.1.0.beta3 of the `beta` and `tests-passed` branches, a user logged as an administrator can request backups multiple times, which will eat up all the connections to the DB. If this is done on a site using multisite, then it can affect the whole cluster. The vulnerability is patched in version 3.0.2 of the `stable` branch and version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds.</p> <p><b>CVE ID : CVE-2023-28107</b></p>	<p><a href="https://github.com/discourse/discourse/commit/78a3efa7104eed6dd3ed7a06a71e2705337d9e61">https://github.com/discourse/discourse/commit/78a3efa7104eed6dd3ed7a06a71e2705337d9e61</a>,  <a href="https://github.com/discourse/discourse/pull/20700">https://github.com/discourse/discourse/pull/20700</a>,  <a href="https://github.com/discourse/discourse/security/advisories/GHSA-cp7c-fm4c-6xxx">https://github.com/discourse/discourse/security/advisories/GHSA-cp7c-fm4c-6xxx</a></p>	A-DIS-DISC-050423/600
Affected Version(s): * Up to (including) 3.1.0					

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
Server-Side Request Forgery (SSRF)	17-Mar-2023	8.1	Discourse is an open-source discussion platform. Prior to version 3.1.0.beta3 of the `beta` and `tests-passed` branches, some user provided URLs were being passed to FastImage without SSRF protection. Insufficient protections could enable attackers to trigger outbound network connections from the Discourse server to private IP addresses. This affects any site running the `tests-passed` or `beta` branches versions 3.1.0.beta2 and prior. This issue is patched in version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds. <b>CVE ID : CVE-2023-28112</b>	<a href="https://github.com/discourse/discourse/pull/20710">https://github.com/discourse/discourse/pull/20710</a> , <a href="https://github.com/discourse/discourse/security/advisories/GHSA-9897-x229-55gh">https://github.com/discourse/discourse/security/advisories/GHSA-9897-x229-55gh</a> , <a href="https://github.com/discourse/discourse/commit/39c2f63b35d90ebaf67b9604cf1d424e5984203c">https://github.com/discourse/discourse/commit/39c2f63b35d90ebaf67b9604cf1d424e5984203c</a>	A-DIS-DISC-050423/601
Affected Version(s): 1.3.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a	<a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a> , <a href="https://github.com/discourse/discourse/commit/105f">https://github.com/discourse/discourse/commit/105f</a>	A-DIS-DISC-050423/602

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
			<p>count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>	<p>ee978d73b0ec23ff814a09d1c0c9ace95164,  <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a</p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a>,  <a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a></p>	A-DIS-DISC-050423/603

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
			<p>count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>	discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7	
Affected Version(s): 1.4.0					
N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in</p>	<p><a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a>,  <a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9</a></p>	A-DIS-DISC-050423/604

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
			<p>a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>	<p>ace95164,  <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the</p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a>,  <a href="https://github.com/discourse/discourse/security/advisories">https://github.com/discourse/discourse/security/advisories</a></p>	A-DIS-DISC-050423/605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>	ories/GHSA-rf8j-mf8c-82v7	
Affected Version(s): 1.5.0					
N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can</p>	<p><a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a>,  <a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164</a>,  <a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a></p>	A-DIS-DISC-050423/606

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>	<p>scourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</p>	
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users</p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a>,  <a href="https://github.com/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a></p>	A-DIS-DISC-050423/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>		

Affected Version(s): 1.6.0

N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new</p>	<p><a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a>,  <a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164</a>,  <a href="https://github.com/discourse/discourse/commit/ecb9">https://github.com/discourse/discourse/commit/ecb9</a></p>	A-DIS-DISC-050423/608
-----	-------------	-----	--	--	-----------------------

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
			<p>topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>	aa5dba947 41d9579f4f 873f0675f4 8b4184f	
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new</p>	<a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a> , <a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a>	A-DIS-DISC-050423/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>		

Affected Version(s): 1.7.0

N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have</p>	<p><a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a>,  <a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164</a>,  <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f</a></p>	A-DIS-DISC-050423/610
-----	-------------	-----	--	--	-----------------------

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>	873f0675f48b4184f	
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have</p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a>,  <a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a></p>	A-DIS-DISC-050423/611

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
			<p>access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>		

Affected Version(s): 1.8.0

N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version</p>	<p><a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a>,  <a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164</a>,  <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	A-DIS-DISC-050423/612
-----	-------------	-----	---	--	-----------------------

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
			<p>3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>		
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the</p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a>,  <a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a></p>	A-DIS-DISC-050423/613

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
			<p>count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>		
Affected Version(s): 1.9.0					
N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the</p>	<p><a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a>,  <a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164</a>,  <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	A-DIS-DISC-050423/614

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
			<p>count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>		
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden</p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a>,  <a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a></p>	A-DIS-DISC-050423/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>		
Affected Version(s): 2.0.0					
N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only</p>	<p><a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a>,  <a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164</a>,  <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	A-DIS-DISC-050423/616

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
			<p>counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>		
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of</p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a>,  <a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a></p>	A-DIS-DISC-050423/617

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
			<p>personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>		
Affected Version(s): 2.1.0					
N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted</p>	<p><a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a>,  <a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164</a>,  <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	A-DIS-DISC-050423/618

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
			<p>categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>		
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the</p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a>,  <a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a></p>	A-DIS-DISC-050423/619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>`display_personal_mes sages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023- 23935</b></p>		
Affected Version(s): 2.2.0					
N/A	17-Mar-2023	4.3	<p>Discourse is an open- source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests- passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests- passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics</p>	<p><a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a>, <a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164</a>, <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	A-DIS-DISC-050423/620

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
			regardless of the topic's category read restrictions. <b>CVE ID : CVE-2023-23622</b>		
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.	<a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a> , <a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a>	A-DIS-DISC-050423/621

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
			<b>CVE ID : CVE-2023-23935</b>		
Affected Version(s): 2.3.0					
N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p>	<p><a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a>,  <a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164</a>,  <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	A-DIS-DISC-050423/622

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
			<b>CVE ID : CVE-2023-23622</b>		
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a>,  <a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a></p>	A-DIS-DISC-050423/623
Affected Version(s): 2.4.0					

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	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>	<p><a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a>,  <a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164</a>,  <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	A-DIS-DISC-050423/624

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a>,  <a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a></p>	A-DIS-DISC-050423/625
Affected Version(s): 2.5.0					
N/A	17-Mar-2023	4.3	Discourse is an open-source discussion	<a href="https://github.com/discourse/discourse">https://github.com/discourse/discourse</a>	A-DIS-DISC-050423/626

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
			<p>platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>	<p>scourse/discourse/pull/20004,  <a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164</a>,  <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions</p>	<p><a href="https://github.com/discourse/discourse/">https://github.com/discourse/discourse/</a></p>	A-DIS-DISC-050423/627

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
			<p>3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>	<p>course/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37, <a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a></p>	
Affected Version(s): 2.6.0					
N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and</p>	<p><a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a>,</p>	A-DIS-DISC-050423/628

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
			<p>version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>	<p><a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164</a>,  <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2</p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43">https://github.com/discourse/discourse/commit/f31f0b70f82c43</a></p>	A-DIS-DISC-050423/629

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>	<p>d93220ce6fc0d4f57440452f37, <a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a></p>	
Affected Version(s): 2.7.0					
N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the</p>	<p><a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a>, <a href="https://github.com/discourse/discourse/">https://github.com/discourse/</a></p>	A-DIS-DISC-050423/630

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
			<p>count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>	<p>course/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164,  <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of</p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a>,</p>	A-DIS-DISC-050423/631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>	<a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a>	

Affected Version(s): 2.8.0

N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular</p>	<a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a> , <a href="https://github.com/discourse/discourse/commit/105fee978d73b">https://github.com/discourse/discourse/commit/105fee978d73b</a>	A-DIS-DISC-050423/632
-----	-------------	-----	--	--	-----------------------

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
			<p>topics regardless of whether the topic is in a read restricted category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have excess to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>	<p>0ec23ff814 a09d1c0c9 ace95164, <a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a></p>	
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal</p>	<p><a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a>, <a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a>,</p>	A-DIS-DISC-050423/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>	course/security/advisories/GHSA-rf8j-mf8c-82v7	
Affected Version(s): 2.9.0					
N/A	17-Mar-2023	4.3	<p>Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag is a count of all regular topics regardless of whether the topic is in a read restricted</p>	<a href="https://github.com/discourse/discourse/pull/20004">https://github.com/discourse/discourse/pull/20004</a> , <a href="https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164">https://github.com/discourse/discourse/commit/105fee978d73b0ec23ff814a09d1c0c9ace95164</a> ,	A-DIS-DISC-050423/634

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
			<p>category or not. As a result, any users can technically poll a sensitive tag to determine if a new topic is created in a category which the user does not have access to. In version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, the count of topics displayed for a tag defaults to only counting regular topics which are not in read restricted categories. Staff users will continue to see a count of all topics regardless of the topic's category read restrictions.</p> <p><b>CVE ID : CVE-2023-23622</b></p>	<a href="https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f">https://github.com/discourse/discourse/commit/ecb9aa5dba94741d9579f4f873f0675f48b4184f</a>	
N/A	16-Mar-2023	4.3	<p>Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta` and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is</p>	<a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6fc0d4f57440452f37</a> , <a href="https://github.com/discourse/discourse/security/advisories/GHSA">https://github.com/discourse/discourse/security/advisories/GHSA</a>	A-DIS-DISC-050423/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>	-rf8j-mf8c-82v7	
Affected Version(s): 3.1.0					
Server-Side Request Forgery (SSRF)	17-Mar-2023	8.1	<p>Discourse is an open-source discussion platform. Prior to version 3.1.0.beta3 of the `beta` and `tests-passed` branches, some user provided URLs were being passed to FastImage without SSRF protection. Insufficient protections could enable attackers to trigger outbound network connections from the Discourse</p>	<p><a href="https://github.com/discourse/discourse/pull/20710">https://github.com/discourse/discourse/pull/20710</a>,  <a href="https://github.com/discourse/discourse/security/advisories/GHSA-9897-x229-55gh">https://github.com/discourse/discourse/security/advisories/GHSA-9897-x229-55gh</a>,  <a href="https://github.com/discourse/discourse/co">https://github.com/discourse/co</a></p>	A-DIS-DISC-050423/636

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
			server to private IP addresses. This affects any site running the `tests-passed` or `beta` branches versions 3.1.0.beta2 and prior. This issue is patched in version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds. <b>CVE ID : CVE-2023-28112</b>	mmit/39c2f63b35d90ebaf67b9604cf1d424e5984203c	
Server-Side Request Forgery (SSRF)	17-Mar-2023	7.5	Discourse is an open-source discussion platform. Prior to version 3.1.0.beta3 of the `beta` and `tests-passed` branches, attackers are able to bypass Discourse's server-side request forgery (SSRF) protection for private IPv4 addresses by using a IPv4-mapped IPv6 address. The issue is patched in the latest beta and tests-passed version of Discourse. version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds. <b>CVE ID : CVE-2023-28111</b>	<a href="https://github.com/discourse/discourse/pull/20710">https://github.com/discourse/discourse/pull/20710</a> , <a href="https://github.com/discourse/discourse/security/advisories/GHSA-26h3-8ww8-v5fc">https://github.com/discourse/discourse/security/advisories/GHSA-26h3-8ww8-v5fc</a> , <a href="https://github.com/discourse/discourse/commit/fd16eade7fcc6bba4b71e71106a2eb13cdfdae4a">https://github.com/discourse/discourse/commit/fd16eade7fcc6bba4b71e71106a2eb13cdfdae4a</a>	A-DIS-DISC-050423/637
Improper Neutralization of	17-Mar-2023	6.1	Discourse is an open-source discussion platform. Between	<a href="https://github.com/discourse/dis">https://github.com/discourse/dis</a>	A-DIS-DISC-050423/638

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			versions 3.1.0.beta2 and 3.1.0.beta3 of the `tests-passed` branch, editing or responding to a chat message containing malicious content could lead to a cross-site scripting attack. This issue is patched in version 3.1.0.beta3 of the `tests-passed` branch. There are no known workarounds. <b>CVE ID : CVE-2023-26040</b>	course/commit/a373bf2a01488c206e7feb28a9d2361b22ce6e70, <a href="https://github.com/discourse/discourse/security/advisories/GHSA-ccfc-qpmp-gq87">https://github.com/discourse/discourse/security/advisories/GHSA-ccfc-qpmp-gq87</a>	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Mar-2023	5.4	Discourse is an open-source discussion platform. Prior to version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches, a maliciously crafted URL can be included in a user's full name field to carry out cross-site scripting attacks on sites with a disabled or overly permissive CSP (Content Security Policy). Discourse's default CSP prevents this vulnerability. The vulnerability is patched in version 3.0.1 of the `stable` branch and version 3.1.0.beta2 of the `beta` and `tests-passed` branches. As a	<a href="https://github.com/discourse/discourse/commit/1a5a6f66cb821ed29a737311d6fdc2eba5adc915">https://github.com/discourse/discourse/commit/1a5a6f66cb821ed29a737311d6fdc2eba5adc915</a> , <a href="https://github.com/discourse/discourse/security/advisories/GHSA-7pm2-prxw-wrvp">https://github.com/discourse/discourse/security/advisories/GHSA-7pm2-prxw-wrvp</a> , <a href="https://github.com/discourse/discourse/pull/20008">https://github.com/discourse/discourse/pull/20008</a>	A-DIS-DISC-050423/639

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
			workaround, enable and/or restore your site's CSP to the default one provided with Discourse. <b>CVE ID : CVE-2023-25172</b>		
Allocation of Resources Without Limits or Throttling	17-Mar-2023	4.9	Discourse is an open-source discussion platform. Prior to version 3.0.2 of the `stable` branch and version 3.1.0.beta3 of the `beta` and `tests-passed` branches, a user logged as an administrator can request backups multiple times, which will eat up all the connections to the DB. If this is done on a site using multisite, then it can affect the whole cluster. The vulnerability is patched in version 3.0.2 of the `stable` branch and version 3.1.0.beta3 of the `beta` and `tests-passed` branches. There are no known workarounds. <b>CVE ID : CVE-2023-28107</b>	<a href="https://github.com/discourse/discourse/commit/78a3efa7104eed6dd3ed7a06a71e2705337d9e61">https://github.com/discourse/discourse/commit/78a3efa7104eed6dd3ed7a06a71e2705337d9e61</a> , <a href="https://github.com/discourse/discourse/pull/20700">https://github.com/discourse/discourse/pull/20700</a> , <a href="https://github.com/discourse/discourse/security/advisories/GHSA-cp7c-fm4c-6xxx">https://github.com/discourse/discourse/security/advisories/GHSA-cp7c-fm4c-6xxx</a>	A-DIS-DISC-050423/640
N/A	16-Mar-2023	4.3	Discourse is an open-source messaging platform. In versions 3.0.1 and prior on the `stable` branch and versions 3.1.0.beta2 and prior on the `beta`	<a href="https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6">https://github.com/discourse/discourse/commit/f31f0b70f82c43d93220ce6</a>	A-DIS-DISC-050423/641

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
			<p>and `tests-passed` branches, the count of personal messages displayed for a tag is a count of all personal messages regardless of whether the personal message is visible to a given user. As a result, any users can technically poll a sensitive tag to determine if a new personal message is created even if the user does not have access to the personal message. In the patched versions, the count of personal messages tagged with a given tag is hidden by default. To revert to the old behaviour of displaying the count of personal messages for a given tag, an admin may enable the `display_personal_messages_tag_counts` site setting.</p> <p><b>CVE ID : CVE-2023-23935</b></p>	<p>fc0d4f57440452f37,  <a href="https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7">https://github.com/discourse/discourse/security/advisories/GHSA-rf8j-mf8c-82v7</a></p>	

**Vendor: dreamer cms project**

**Product: dreamer cms**

Affected Version(s): 4.0.1

Incorrect Permission Assignment for Critical Resource	16-Mar-2023	5.3	Permissions vulnerability found in isoftforce Dreamer CMS v.4.0.1 allows local attackers to obtain sensitive	N/A	A-DRE-DREA-050423/642
---	-------------	-----	--	-----	-----------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information via the AttachmentController parameter. <b>CVE ID : CVE-2023-27084</b>		
<b>Vendor: e-commerce_system_project</b>					
<b>Product: e-commerce_system</b>					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester E-Commerce System 1.0. This issue affects some unknown processing of the file /ecommerce/admin/settings/setDiscount.php. The manipulation of the argument id with the input 201737 AND (SELECT 8973 FROM (SELECT(SLEEP(5)))OAD) leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223409 was assigned to this vulnerability. <b>CVE ID : CVE-2023-1505</b>	N/A	A-E-C-E-CO-050423/643
Improper Neutralization of Special Elements	20-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester E-Commerce System 1.0.	N/A	A-E-C-E-CO-050423/644

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			Affected is an unknown function of the file login.php. The manipulation of the argument U_USERNAME leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-223410 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1506</b>		
Improper Access Control	22-Mar-2023	9.8	A vulnerability was found in SourceCodester E-Commerce System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /ecommerce/admin/user/controller.php?action=edit of the component Username Handler. The manipulation of the argument USERID leads to improper access controls. The attack may be launched remotely. VDB-223550 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1557</b>	N/A	A-E-C-E-CO-050423/645

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')	20-Mar-2023	6.1	A vulnerability has been found in SourceCodester E-Commerce System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /ecommerce/admin/category/controller.php of the component Category Name Handler. The manipulation of the argument CATEGORY leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223411. <b>CVE ID : CVE-2023-1507</b>	N/A	A-E-C-E-CO-050423/646
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A vulnerability classified as problematic was found in SourceCodester E-Commerce System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/user/controller.php?action=edit. The manipulation of the argument U_NAME with the input	N/A	A-E-C-E-CO-050423/647

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>&lt;script&gt;alert('1')&lt;/script&gt; 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-223561 was assigned to this vulnerability.</p> <p><b>CVE ID : CVE-2023-1569</b></p>		
<b>Vendor: e-dynamics</b>					
<b>Product: events_made_easy</b>					
Affected Version(s): * Up to (including) 2.3.14					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8.8	<p>The Events Made Easy WordPress Plugin, version &lt;= 2.3.14 is affected by an authenticated SQL injection vulnerability in the 'search_name' parameter in the eme_recurrences_list action.</p> <p><b>CVE ID : CVE-2023-28660</b></p>	N/A	A-E-D-EVEN-050423/648
<b>Vendor: earnings_and_expense_tracker_application_project</b>					
<b>Product: earnings_and_expense_tracker_application</b>					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Mar-2023	6.1	<p>A vulnerability classified as problematic has been found in SourceCodester Earnings and Expense Tracker App 1.0. This affects an unknown part of the file Master.php?a=save_ex</p>	N/A	A-EAR-EARN-050423/649

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
			<p>pense. The manipulation of the argument name leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-224307.</p> <p><b>CVE ID : CVE-2023-1688</b></p>		
<b>Vendor: earnings_and_expense_tracker_app_project</b>					
<b>Product: earnings_and_expense_tracker_app</b>					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Mar-2023	6.1	<p>A vulnerability classified as problematic was found in SourceCodester Earnings and Expense Tracker App 1.0. This vulnerability affects unknown code of the file Master.php?a=save_earning. The manipulation of the argument name leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-224308.</p> <p><b>CVE ID : CVE-2023-1689</b></p>	N/A	A-EAR-EARN-050423/650
<b>Vendor: ellucian</b>					
<b>Product: banner_web_tailor</b>					
Affected Version(s): 8.6					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	25-Mar-2023	8.8	<p><b>** DISPUTED **</b> A vulnerability has been found in Ellucian Banner Web Tailor 8.6 and classified as critical. This vulnerability affects unknown code of the file /PROD_ar/twbkwbis.P_FirstMenu of the component Login Page. The manipulation of the argument PIDM/WEBID leads to improper authorization. The attack can be initiated remotely. After submitting proper login credentials it becomes possible to generate new valid session identifiers on the OTP page. The real existence of this vulnerability is still doubted at the moment. VDB-224014 is the identifier assigned to this vulnerability.</p> <p><b>CVE ID : CVE-2023-1632</b></p>	N/A	A-ELL-BANN-050423/651
<b>Vendor: evilmartians</b>					
<b>Product: imgproxy</b>					
Affected Version(s): * Up to (excluding) 3.14.0					
Improper Neutralization of Input	19-Mar-2023	5.4	Cross-site Scripting (XSS) - Reflected in GitHub repository	<a href="https://hunter.dev/boonties/de603972-">https://hunter.dev/boonties/de603972-</a>	A-EVI-IMGP-050423/652

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			imgproxy/imgproxy prior to 3.14.0. <b>CVE ID : CVE-2023-1496</b>	935a-401a-96fb-17ddadd282b2, <a href="https://github.com/imgproxy/imgproxy/commit/62f8d08a93d301285dcd1dabcc7ba10c6c65b689">https://github.com/imgproxy/imgproxy/commit/62f8d08a93d301285dcd1dabcc7ba10c6c65b689</a>	
<b>Vendor: evolucionare</b>					
<b>Product: ecs_imaging</b>					
Affected Version(s): 6.21.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	<b>** UNSUPPORTED WHEN ASSIGNED **</b> EVOLUCARE ECSIMAGING (aka ECS Imaging) < 6.21.5 is vulnerable to Cross Site Scripting (XSS) via new_movie.php. <b>CVE ID : CVE-2023-26913</b>	N/A	A-EVO-ECS_-050423/653
<b>Vendor: Extplorer</b>					
<b>Product: extplorer</b>					
Affected Version(s): 2.1.15					
N/A	21-Mar-2023	8.8	Insecure Permissions vulnerability found in Extplorer File manager eXtplorer v.2.1.15 allows a remote attacker to execute arbitrary code via the index.php component	N/A	A-EXT-EXTP-050423/654

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-27842</b>		
<b>Vendor: Fedoraproject</b>					
<b>Product: extra_packages_for_enterprise_linux</b>					
Affected Version(s): 8.0					
Improper Input Validation	23-Mar-2023	5.5	<p>A vulnerability was discovered in ImageMagick where a specially created SVG file loads itself and causes a segmentation fault. This flaw allows a remote attacker to pass a specially crafted SVG file that leads to a segmentation fault, generating many trash files in "/tmp," resulting in a denial of service. When ImageMagick crashes, it generates a lot of trash files. These trash files can be large if the SVG file contains many render actions. In a denial of service attack, if a remote attacker uploads an SVG file of size t, ImageMagick generates files of size 103*t. If an attacker uploads a 100M SVG, the server will generate about 10G.</p> <p><b>CVE ID : CVE-2023-1289</b></p>	<p><a href="https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4">https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4</a>,  <a href="https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr">https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr</a>,  <a href="https://bugzilla.redhat.com/show_bug.cgi?id=2176858">https://bugzilla.redhat.com/show_bug.cgi?id=2176858</a></p>	A-FED-EXTR-050423/655
Affected Version(s): 9.0					

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 Input Validation	23-Mar-2023	5.5	<p>A vulnerability was discovered in ImageMagick where a specially created SVG file loads itself and causes a segmentation fault. This flaw allows a remote attacker to pass a specially crafted SVG file that leads to a segmentation fault, generating many trash files in "/tmp," resulting in a denial of service. When ImageMagick crashes, it generates a lot of trash files. These trash files can be large if the SVG file contains many render actions. In a denial of service attack, if a remote attacker uploads an SVG file of size t, ImageMagick generates files of size 103*t. If an attacker uploads a 100M SVG, the server will generate about 10G.</p> <p><b>CVE ID : CVE-2023-1289</b></p>	<p><a href="https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4">https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4</a>,  <a href="https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr">https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr</a>,  <a href="https://bugzilla.redhat.com/show_bug.cgi?id=2176858">https://bugzilla.redhat.com/show_bug.cgi?id=2176858</a></p>	A-FED-EXTR-050423/656
<b>Vendor: feifeicms</b>					
<b>Product: feifeicms</b>					
Affected Version(s): 2.7.130201					
Improper Neutralization of Input During	22-Mar-2023	5.4	<p>A vulnerability was found in FeiFeiCMS 2.7.130201. It has been classified as problematic. This</p>	N/A	A-FEI-FEIF-050423/657

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			affects an unknown part of the file \Public\system\slide_add.html of the component Extension Tool. 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-223557 was assigned to this vulnerability. <b>CVE ID : CVE-2023-1565</b>		
<b>Vendor: file_management_system_project</b>					
<b>Product: file_management_system</b>					
Affected Version(s): 1.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	A cross-site scripting (XSS) vulnerability in File Management Project 1.0.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field under the Edit User module. <b>CVE ID : CVE-2023-27245</b>	<a href="https://github.com/flyasolo/File-Management-System">https://github.com/flyasolo/File-Management-System</a>	A-FIL-FILE-050423/658
<b>Vendor: Filseclab</b>					
<b>Product: twister_antivirus</b>					
Affected Version(s): 8.0					
Improper Resource Shutdown or Release	17-Mar-2023	7.5	A vulnerability was found in Filseclab Twister Antivirus 8. It has been declared as problematic. This	N/A	A-FIL-TWIS-050423/659

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
			<p>vulnerability affects the function 0x80112053 in the library fildds.sys of the component IoControlCode 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. The identifier of this vulnerability is VDB-223288.</p> <p><b>CVE ID : CVE-2023-1443</b></p>		
NULL Pointer Dereference	17-Mar-2023	6.5	<p>A vulnerability was found in Filseclab Twister Antivirus 8. It has been rated as critical. This issue affects the function 0x8011206B in the library fildds.sys of the component IoControlCode 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-223289 was assigned to this vulnerability.</p> <p><b>CVE ID : CVE-2023-1444</b></p>	N/A	A-FIL-TWIS-050423/660

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 Resource Shutdown or Release	17-Mar-2023	5.5	A vulnerability classified as problematic has been found in Filseclab Twister Antivirus 8. Affected is the function 0x80112053 in the library fildds.sys of the component IoControlCode Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. VDB-223290 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1445</b>	N/A	A-FIL-TWIS-050423/661

**Vendor: fit2cloud**

**Product: jumpserver**

Affected Version(s): \* Up to (excluding) 2.28.8

Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Mar-2023	9.9	Jumpserver is a popular open source bastion host, and Koko is a Jumpserver component that is the Go version of coco, refactoring coco's SSH/SFTP service and Web Terminal service. Prior to version 2.28.8, using illegal tokens to connect to a Kubernetes cluster through Koko can result in the execution	<a href="https://github.com/jumpserver/jumpserver/security/advisories/GHSA-6x5p-jm59-jh29">https://github.com/jumpserver/jumpserver/security/advisories/GHSA-6x5p-jm59-jh29</a> , <a href="https://github.com/jumpserver/jumpserver/releases/tag/v2.28.8">https://github.com/jumpserver/jumpserver/releases/tag/v2.28.8</a>	A-FIT-JUMP-050423/662
---	-------------	-----	--	---	-----------------------

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
			of dangerous commands that may disrupt the Koko container environment and affect normal usage. The vulnerability has been fixed in v2.28.8. <b>CVE ID : CVE-2023-28110</b>		
<b>Product: koko</b>					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Mar-2023	9.9	Jumpserver is a popular open source bastion host, and Koko is a Jumpserver component that is the Go version of coco, refactoring coco's SSH/SFTP service and Web Terminal service. Prior to version 2.28.8, using illegal tokens to connect to a Kubernetes cluster through Koko can result in the execution of dangerous commands that may disrupt the Koko container environment and affect normal usage. The vulnerability has been fixed in v2.28.8. <b>CVE ID : CVE-2023-28110</b>	<a href="https://github.com/jumpserver/jumpserver/security/advisories/GHSA-6x5p-jm59-jh29">https://github.com/jumpserver/jumpserver/security/advisories/GHSA-6x5p-jm59-jh29</a> , <a href="https://github.com/jumpserver/jumpserver/releases/tag/v2.28.8">https://github.com/jumpserver/releases/tag/v2.28.8</a>	A-FIT-KOKO-050423/663
<b>Vendor: Flatpak</b>					
<b>Product: Flatpak</b>					
Affected Version(s): From (including) 1.12.0 Up to (excluding) 1.12.8					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	16-Mar-2023	4.3	<p>Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. In versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4, if an attacker publishes a Flatpak app with elevated permissions, they can hide those permissions from users of the `flatpak(1)` command-line interface by setting other permissions to crafted values that contain non-printable control characters such as `ESC`. A fix is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, use a GUI like GNOME Software rather than the command-line interface, or only install apps whose maintainers you trust.</p> <p><b>CVE ID : CVE-2023-28101</b></p>	<p><a href="https://github.com/flatpak/flatpak/commit/6cac99daffe6003c8a4bd5666341c217876536869">https://github.com/flatpak/flatpak/commit/6cac99daffe6003c8a4bd5666341c217876536869</a>,  <a href="https://github.com/flatpak/flatpak/commit/7fe63f2e8f1fd2dafc31d45154cf0b191ebec66c">https://github.com/flatpak/flatpak/commit/7fe63f2e8f1fd2dafc31d45154cf0b191ebec66c</a>,  <a href="https://github.com/flatpak/flatpak/commit/409e34187de2b2b2c4ef34c79f417be698830f6c">https://github.com/flatpak/flatpak/commit/409e34187de2b2b2c4ef34c79f417be698830f6c</a></p>	A-FLA-FLAT-050423/664
N/A	16-Mar-2023	10	<p>Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. Versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4 contain a vulnerability similar</p>	<p><a href="https://github.com/flatpak/flatpak/security/advisories/GHSA-7qpw-3vjv-xrqp">https://github.com/flatpak/flatpak/security/advisories/GHSA-7qpw-3vjv-xrqp</a>,  <a href="https://github.com/flatpak/flatpak/security/advisories/GHSA-7qpw-3vjv-xrqp">https://github.com/flatpak/flatpak/security/advisories/GHSA-7qpw-3vjv-xrqp</a></p>	A-FLA-FLAT-050423/665

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
			<p>to CVE-2017-5226, but using the `TIOCLINUX` ioctl command instead of `TIOCSTI`. If a Flatpak app is run on a Linux virtual console such as `/dev/tty1`, it can copy text from the virtual console and paste it into the command buffer, from which the command might be run after the Flatpak app has exited. Ordinary graphical terminal emulators like xterm, gnome-terminal and Konsole are unaffected. This vulnerability is specific to the Linux virtual consoles `/dev/tty1`, `/dev/tty2` and so on. A patch is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, don't run Flatpak on a Linux virtual console. Flatpak is primarily designed to be used in a Wayland or X11 graphical environment.</p> <p><b>CVE ID : CVE-2023-28100</b></p>	<a href="https://github.com/flatpak/flatpak/commit/8e63de9a7d3124f91140fc74f8ca9ed73ed53be9">hub.com/flatpak/flatpak/commit/8e63de9a7d3124f91140fc74f8ca9ed73ed53be9</a>	
Affected Version(s): * Up to (excluding) 1.10.8					
Improper Encoding or	16-Mar-2023	4.3	Flatpak is a system for building, distributing, and running	<a href="https://github.com/flatpak/flatpak">https://github.com/flatpak/flatpak</a>	A-FLA-FLAT-050423/666

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Escaping of Output			sandboxed desktop applications on Linux. In versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4, if an attacker publishes a Flatpak app with elevated permissions, they can hide those permissions from users of the `flatpak(1)` command-line interface by setting other permissions to crafted values that contain non-printable control characters such as `ESC`. A fix is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, use a GUI like GNOME Software rather than the command-line interface, or only install apps whose maintainers you trust. <b>CVE ID : CVE-2023-28101</b>	ak/commit /6cac99daf e6003c8a4 bd5666341 c21787653 6869, <a href="https://github.com/flatpak/flatpak/commit/7fe63f2e8f1fd2dafc31d45154cf0b191ebec66c">https://github.com/flatpak/flatpak/commit/7fe63f2e8f1fd2dafc31d45154cf0b191ebec66c</a> , <a href="https://github.com/flatpak/flatpak/commit/409e34187de2b2b2c4ef34c79f417be698830f6c">https://github.com/flatpak/flatpak/commit/409e34187de2b2b2c4ef34c79f417be698830f6c</a>	
N/A	16-Mar-2023	10	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. Versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4 contain a vulnerability similar to CVE-2017-5226, but using the `TIOCLINUX` ioctl	<a href="https://github.com/flatpak/flatpak/security/advisories/GHSA-7qpw-3vjv-xrqp">https://github.com/flatpak/flatpak/security/advisories/GHSA-7qpw-3vjv-xrqp</a> , <a href="https://github.com/flatpak/flatpak/commit">https://github.com/flatpak/flatpak/commit</a>	A-FLA-FLAT-050423/667

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
			<p>command instead of `TIOCSTI`. If a Flatpak app is run on a Linux virtual console such as `/dev/tty1`, it can copy text from the virtual console and paste it into the command buffer, from which the command might be run after the Flatpak app has exited. Ordinary graphical terminal emulators like xterm, gnome-terminal and Konsole are unaffected. This vulnerability is specific to the Linux virtual consoles `/dev/tty1`, `/dev/tty2` and so on. A patch is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, don't run Flatpak on a Linux virtual console. Flatpak is primarily designed to be used in a Wayland or X11 graphical environment.</p> <p><b>CVE ID : CVE-2023-28100</b></p>	/8e63de9a 7d3124f91 140fc74f8c a9ed73ed5 3be9	
Affected Version(s): From (including) 1.14.0 Up to (excluding) 1.14.4					
Improper Encoding or Escaping of Output	16-Mar-2023	4.3	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. In versions prior to	<a href="https://github.com/flatpak/flatpak/commit/6cac99daf6003c8a4">https://github.com/flatpak/flatpak/commit/6cac99daf6003c8a4</a>	A-FLA-FLAT-050423/668

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
			<p>1.10.8, 1.12.8, 1.14.4, and 1.15.4, if an attacker publishes a Flatpak app with elevated permissions, they can hide those permissions from users of the `flatpak(1)` command-line interface by setting other permissions to crafted values that contain non-printable control characters such as `ESC`. A fix is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, use a GUI like GNOME Software rather than the command-line interface, or only install apps whose maintainers you trust.</p> <p><b>CVE ID : CVE-2023-28101</b></p>	<p>bd5666341c217876536869,  <a href="https://github.com/flatpak/flatpak/commit/7fe63f2e8f1fd2dafc31d45154cf0b191e6c66c">https://github.com/flatpak/flatpak/commit/7fe63f2e8f1fd2dafc31d45154cf0b191e6c66c</a>,  <a href="https://github.com/flatpak/flatpak/commit/409e34187de2b2b2c4ef34c79f417be698830f6c">https://github.com/flatpak/flatpak/commit/409e34187de2b2b2c4ef34c79f417be698830f6c</a></p>	
N/A	16-Mar-2023	10	<p>Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. Versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4 contain a vulnerability similar to CVE-2017-5226, but using the `TIOCLINUX` ioctl command instead of `TIOCSTI`. If a Flatpak app is run on a Linux</p>	<p><a href="https://github.com/flatpak/flatpak/security/advisories/GHSA-7qpw-3vjv-xrqp">https://github.com/flatpak/flatpak/security/advisories/GHSA-7qpw-3vjv-xrqp</a>,  <a href="https://github.com/flatpak/flatpak/commit/8e63de9a7d3124f91140fc74f8c">https://github.com/flatpak/flatpak/commit/8e63de9a7d3124f91140fc74f8c</a></p>	A-FLA-FLAT-050423/669

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
			<p>virtual console such as <code>/dev/tty1`</code>, it can copy text from the virtual console and paste it into the command buffer, from which the command might be run after the Flatpak app has exited. Ordinary graphical terminal emulators like xterm, gnome-terminal and Konsole are unaffected. This vulnerability is specific to the Linux virtual consoles <code>/dev/tty1`</code>, <code>/dev/tty2`</code> and so on. A patch is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, don't run Flatpak on a Linux virtual console. Flatpak is primarily designed to be used in a Wayland or X11 graphical environment.</p> <p><b>CVE ID : CVE-2023-28100</b></p>	a9ed73ed53be9	
Affected Version(s): From (including) 1.15.0 Up to (excluding) 1.15.4					
Improper Encoding or Escaping of Output	16-Mar-2023	4.3	<p>Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. In versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4, if an attacker publishes a</p>	<a href="https://github.com/flatpak/flatpak/commit/6cac99daf6003c8a4bd5666341c217876536869">https://github.com/flatpak/flatpak/commit/6cac99daf6003c8a4bd5666341c217876536869,</a>	A-FLA-FLAT-050423/670

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
			<p>Flatpak app with elevated permissions, they can hide those permissions from users of the `flatpak(1)` command-line interface by setting other permissions to crafted values that contain non-printable control characters such as `ESC`. A fix is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, use a GUI like GNOME Software rather than the command-line interface, or only install apps whose maintainers you trust.</p> <p><b>CVE ID : CVE-2023-28101</b></p>	<p><a href="https://github.com/flatpak/flatpak/commit/7fe63f2e8f1fd2dafc31d45154cf0b191e6c66c">https://github.com/flatpak/flatpak/commit/7fe63f2e8f1fd2dafc31d45154cf0b191e6c66c</a>,  <a href="https://github.com/flatpak/flatpak/commit/409e34187de2b2b2c4ef34c79f417be698830f6c">https://github.com/flatpak/flatpak/commit/409e34187de2b2b2c4ef34c79f417be698830f6c</a></p>	
N/A	16-Mar-2023	10	<p>Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. Versions prior to 1.10.8, 1.12.8, 1.14.4, and 1.15.4 contain a vulnerability similar to CVE-2017-5226, but using the `TIOCLINUX` ioctl command instead of `TIOCSTI`. If a Flatpak app is run on a Linux virtual console such as `/dev/tty1`, it can copy text from the</p>	<p><a href="https://github.com/flatpak/flatpak/security/advisories/GHSA-7qpw-3vjv-xrqp">https://github.com/flatpak/flatpak/security/advisories/GHSA-7qpw-3vjv-xrqp</a>,  <a href="https://github.com/flatpak/flatpak/commit/8e63de9a7d3124f91140fc74f8ca9ed73ed53be9">https://github.com/flatpak/flatpak/commit/8e63de9a7d3124f91140fc74f8ca9ed73ed53be9</a></p>	A-FLA-FLAT-050423/671

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
			<p>virtual console and paste it into the command buffer, from which the command might be run after the Flatpak app has exited. Ordinary graphical terminal emulators like xterm, gnome-terminal and Konsole are unaffected. This vulnerability is specific to the Linux virtual consoles <code>/dev/tty1</code>, <code>/dev/tty2</code> and so on. A patch is available in versions 1.10.8, 1.12.8, 1.14.4, and 1.15.4. As a workaround, don't run Flatpak on a Linux virtual console. Flatpak is primarily designed to be used in a Wayland or X11 graphical environment.</p> <p><b>CVE ID : CVE-2023-28100</b></p>		

**Vendor: formidablepro2pdf**

**Product: formidable\_pro2pdf**

Affected Version(s): \* Up to (excluding) 3.11

Improper Neutralization of Special Elements used in an SQL Command	22-Mar-2023	8.8	The Formidable PRO2PDF WordPress Plugin, version < 3.11, is affected by an authenticated SQL injection vulnerability in the 'fieldmap' parameter in the	N/A	A-FOR-FORM-050423/672
--	-------------	-----	---	-----	-----------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			fpropdf_export_file action. <b>CVE ID : CVE-2023-28663</b>		
<b>Vendor: gadget_works_online_ordering_system_project</b>					
<b>Product: gadget_works_online_ordering_system</b>					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	16-Mar-2023	7.2	A vulnerability was found in SourceCodester Gadget Works Online Ordering System 1.0. It has been classified as problematic. This affects an unknown part of the file admin/products/controller.php?action=add of the component Products Handler. The manipulation of the argument filename 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-223215. <b>CVE ID : CVE-2023-1433</b>	<a href="https://github.com/zhengjiashe/bug_report/blob/main/UPLOAD.md">https://github.com/zhengjiashe/bug_report/blob/main/UPLOAD.md</a>	A-GAD-GADG-050423/673
<b>Vendor: galaxyproject</b>					
<b>Product: galaxy</b>					
Affected Version(s): * Up to (excluding) 22.01					
Incorrect Authorization	20-Mar-2023	7.5	Galaxy is an open-source platform for data analysis. All supported versions of	<a href="https://github.com/galaxyproject/galaxy">https://github.com/galaxyproject/galaxy/se</a>	A-GAL-GALA-050423/674

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
			<p>Galaxy are affected prior to 22.01, 22.05, and 23.0 are affected by an insufficient permission check. Unsupported versions are likely affected as far back as the functionality of Visualizations/Pages exists. Due to this issue, an attacker can modify or delete any Galaxy Visualization or Galaxy Page given they know the encoded ID of it. Additionally, they can copy or import any Galaxy Visualization given they know the encoded ID of it. Patches are available for versions 22.01, 22.05, and 23.0. For the changes to take effect, you must restart all Galaxy server processes. There are no supported workarounds.</p> <p><b>CVE ID : CVE-2023-27578</b></p>	curity/advisories/GHS-A-j8q2-r4g5-f22j	
<b>Vendor: GE</b>					
<b>Product: ifix</b>					
Affected Version(s): 2022					
Improper Control of Generation of Code	16-Mar-2023	9.8	GE Digital Proficy iFIX 2022, GE Digital Proficy iFIX v6.1, and GE Digital Proficy iFIX v6.5 are vulnerable to	N/A	A-GE-IFIX-050423/675

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
('Code Injection')			code injection, which may allow an attacker to insert malicious configuration files in the expected web server execution path and gain full control of the HMI software. <b>CVE ID : CVE-2023-0598</b>		
Affected Version(s): 6.1					
Improper Control of Generation of Code ('Code Injection')	16-Mar-2023	9.8	GE Digital Proficy iFIX 2022, GE Digital Proficy iFIX v6.1, and GE Digital Proficy iFIX v6.5 are vulnerable to code injection, which may allow an attacker to insert malicious configuration files in the expected web server execution path and gain full control of the HMI software. <b>CVE ID : CVE-2023-0598</b>	N/A	A-GE-IFIX-050423/676
Affected Version(s): 6.5					
Improper Control of Generation of Code ('Code Injection')	16-Mar-2023	9.8	GE Digital Proficy iFIX 2022, GE Digital Proficy iFIX v6.1, and GE Digital Proficy iFIX v6.5 are vulnerable to code injection, which may allow an attacker to insert malicious configuration files in the expected web server execution path and gain full control of the HMI software.	N/A	A-GE-IFIX-050423/677

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
			<b>CVE ID : CVE-2023-0598</b>		
<b>Vendor: generalbytes</b>					
<b>Product: crypto_application_server</b>					
Affected Version(s): 20230120					
Unrestricted Upload of File with Dangerous Type	22-Mar-2023	9.1	General Bytes Crypto Application Server (CAS) 20230120, as distributed with General Bytes BATM devices, allows remote attackers to execute arbitrary Java code by uploading a Java application to the /batm/app/admin/standalone/deployments directory, aka BATM-4780, as exploited in the wild in March 2023. This is fixed in 20221118.48 and 20230120.44.  <b>CVE ID : CVE-2023-28725</b>	<a href="https://generalbytes.atlassian.net/wiki/spaces/ESD/pages/2885222430/Security+Incident+March+17-18th+2023">https://generalbytes.atlassian.net/wiki/spaces/ESD/pages/2885222430/Security+Incident+March+17-18th+2023</a>	A-GEN-CRYP-050423/678
<b>Vendor: Gentoo</b>					
<b>Product: soko</b>					
Affected Version(s): * Up to (excluding) 1.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Mar-2023	9.8	Soko if the code that powers packages.gentoo.org. Prior to version 1.0.2, the two package search handlers, `Search` and `SearchFeed`, implemented in `pkg/app/handler/packages/search.go`, are affected by a SQL injection via the `q`	<a href="https://gitweb.gentoo.org/sites/oko.git/commit/?id=4fa6e4b619c0362728955b6ec56eab0e0cbf1e23">https://gitweb.gentoo.org/sites/oko.git/commit/?id=4fa6e4b619c0362728955b6ec56eab0e0cbf1e23</a> , <a href="https://github.com/gentoo/soko">https://github.com/gentoo/soko</a>	A-GEN-SOKO-050423/679

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
			parameter. As a result, unauthenticated attackers can execute arbitrary SQL queries on <code>`https://packages.gentoo.org/`</code> . It was also demonstrated that primitive was enough to gain code execution in the context of the PostgreSQL container. The issue was addressed in commit <code>`4fa6e4b619c0362728955b6ec56eab0e0cbf1e23y`</code> of version 1.0.2 using prepared statements to interpolate user-controlled data in SQL queries. <b>CVE ID : CVE-2023-28424</b>	<a href="#">/security/advisories/GHSA-gc2x-86p3-mxg2</a>	

**Vendor: geosolutionsgroup**

**Product: geonode**

Affected Version(s): \* Up to (excluding) 2.18.7

Exposure of Sensitive Information to an Unauthorized Actor	24-Mar-2023	5.3	GeoNode is an open source platform that facilitates the creation, sharing, and collaborative use of geospatial data. Prior to versions 2.20.6, 2.19.6, and 2.18.7, anonymous users can obtain sensitive information about GeoNode configurations from the response of the <code>`/geoserver/rest/abo</code>	<a href="https://github.com/GeoNode/geonode/security/advisories/GHSA-87mh-vw7c-5v6w">https://github.com/GeoNode/geonode/security/advisories/GHSA-87mh-vw7c-5v6w</a> , <a href="https://github.com/GeoNode/geoserver-geonode-ext/blob/2.">https://github.com/GeoNode/geoserver-geonode-ext/blob/2.</a>	A-GEO-GEON-050423/680
--	-------------	-----	---	---	-----------------------

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
			<p>ut/status` Geoserver REST API endpoint. The Geoserver endpoint is secured by default, but the configuration of Geoserver for GeoNode opens a list of REST endpoints to support some of its public-facing services. The vulnerability impacts both GeoNode 3 and GeoNode 4 instances. Geoserver security configuration is provided by `geoserver-geonode-ext`. A patch for 2.20.7 has been released which blocks access to the affected endpoint. The patch has been backported to branches 2.20.6, 2.19.7, 2.19.6, and 2.18.7. All the published artifacts and Docker images have been updated accordingly. A more advanced patch has been applied to the master and development versions, which require some changes to GeoNode code. They will be available with the next 4.1.0 release. The patched configuration only has an effect on new deployments. For existing setups, the</p>	20.7/data/security/rest.properties	

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
			<p>patch must be applied manually inside the Geoserver data directory. The patched file must replace the existing <code>&lt;geoserver_datadir&gt;/security/rest.properties` file.</code></p> <p><b>CVE ID : CVE-2023-28442</b></p>		
Affected Version(s): From (including) 2.19.0 Up to (excluding) 2.19.6					
Exposure of Sensitive Information to an Unauthorized Actor	24-Mar-2023	5.3	<p>GeoNode is an open source platform that facilitates the creation, sharing, and collaborative use of geospatial data. Prior to versions 2.20.6, 2.19.6, and 2.18.7, anonymous users can obtain sensitive information about GeoNode configurations from the response of the <code>/geoserver/rest/about/status` Geoserver REST API endpoint.</code> The Geoserver endpoint is secured by default, but the configuration of Geoserver for GeoNode opens a list of REST endpoints to support some of its public-facing services. The vulnerability impacts both GeoNode 3 and GeoNode 4 instances. Geoserver security configuration</p>	<p><a href="https://github.com/GeoNode/geonode/security/advisories/GHSA-87mh-vw7c-5v6w">https://github.com/GeoNode/geonode/security/advisories/GHSA-87mh-vw7c-5v6w</a>,  <a href="https://github.com/GeoNode/geonode-geonode-ext/blob/2.20.7/data/security/rest.properties">https://github.com/GeoNode/geonode-geonode-ext/blob/2.20.7/data/security/rest.properties</a></p>	A-GEO-GEON-050423/681

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
			<p>is provided by `geoserver-geonode-ext`. A patch for 2.20.7 has been released which blocks access to the affected endpoint. The patch has been backported to branches 2.20.6, 2.19.7, 2.19.6, and 2.18.7. All the published artifacts and Docker images have been updated accordingly. A more advanced patch has been applied to the master and development versions, which require some changes to GeoNode code. They will be available with the next 4.1.0 release. The patched configuration only has an effect on new deployments. For existing setups, the patch must be applied manually inside the Geoserver data directory. The patched file must replace the existing `<code>&lt;geoserver_datadir&gt;/security/rest.properties` file.</code></p> <p><b>CVE ID : CVE-2023-28442</b></p>		
Affected Version(s): From (including) 2.20.0 Up to (excluding) 2.20.6					
Exposure of Sensitive Informatio	24-Mar-2023	5.3	GeoNode is an open source platform that facilitates the creation,	<a href="https://github.com/GeoNode/geoserver-geonode-ext">https://github.com/GeoNode/geoserver-geonode-ext</a>	A-GEO-GEON-050423/682

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access to an Unauthorized Actor			<p>sharing, and collaborative use of geospatial data. Prior to versions 2.20.6, 2.19.6, and 2.18.7, anonymous users can obtain sensitive information about GeoNode configurations from the response of the <code>`/geoserver/rest/about/status`</code> Geoserver REST API endpoint. The Geoserver endpoint is secured by default, but the configuration of Geoserver for GeoNode opens a list of REST endpoints to support some of its public-facing services. The vulnerability impacts both GeoNode 3 and GeoNode 4 instances. Geoserver security configuration is provided by <code>`geoserver-geonode-ext`</code>. A patch for 2.20.7 has been released which blocks access to the affected endpoint. The patch has been backported to branches 2.20.6, 2.19.7, 2.19.6, and 2.18.7. All the published artifacts and Docker images have been updated accordingly. A more advanced patch has</p>	<p>onode/security/advisories/GHSA-87mh-vw7c-5v6w, <a href="https://github.com/GeoNode/geoserver-geonode-ext/blob/2.20.7/data/security/rest.properties">https://github.com/GeoNode/geoserver-geonode-ext/blob/2.20.7/data/security/rest.properties</a></p>	

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
			<p>been applied to the master and development versions, which require some changes to GeoNode code. They will be available with the next 4.1.0 release. The patched configuration only has an effect on new deployments. For existing setups, the patch must be applied manually inside the Geoserver data directory. The patched file must replace the existing <code>&lt;geoserver_datadir&gt;/security/rest.properties` file.</code></p> <p><b>CVE ID : CVE-2023-28442</b></p>		

**Vendor: getresponse**

**Product: getresponse**

Affected Version(s): \* Up to (excluding) 5.5.31

<p>Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')</p>	20-Mar-2023	5.4	<p>The GetResponse for WordPress plugin through 5.5.31 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.</p>	N/A	A-GET-GETR-050423/683
---	-------------	-----	---	-----	-----------------------

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
			<b>CVE ID : CVE-2023-0167</b>		
<b>Vendor: getshortcodes</b>					
<b>Product: shortcodes_ultimate</b>					
Affected Version(s): * Up to (excluding) 5.12.8					
Missing Authorization	20-Mar-2023	6.5	The WordPress Shortcodes Plugin — Shortcodes Ultimate WordPress plugin before 5.12.8 does not ensure that posts to be displayed via some shortcodes are already public and can be accessed by the user making the request, allowing any authenticated users such as subscriber to view draft, private or even password protected posts. It is also possible to leak the password of protected posts <b>CVE ID : CVE-2023-0890</b>	N/A	A-GET-SHOR-050423/684
Missing Authorization	20-Mar-2023	6.5	The WordPress Shortcodes Plugin — Shortcodes Ultimate WordPress plugin before 5.12.8 does not validate the user meta to be retrieved via the user shortcode, allowing any authenticated users such as subscriber to retrieve arbitrary user meta (except the user_pass), such as the user email and	N/A	A-GET-SHOR-050423/685

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			activation key by default. <b>CVE ID : CVE-2023-0911</b>		
<b>Vendor: gmace_project</b>					
<b>Product: gmace</b>					
Affected Version(s): * Up to (including) 1.5.2					
Cross-Site Request Forgery (CSRF)	29-Mar-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in German Mesky GMACE plugin <= 1.5.2 versions. <b>CVE ID : CVE-2023-23861</b>	N/A	A-GMA-GMAC-050423/686
<b>Vendor: GNU</b>					
<b>Product: org_mode</b>					
Affected Version(s): * Up to (including) 9.6.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Mar-2023	7.8	org-babel-execute:latex in ob-latex.el in Org Mode through 9.6.1 for GNU Emacs allows attackers to execute arbitrary commands via a file name or directory name that contains shell metacharacters. <b>CVE ID : CVE-2023-28617</b>	<a href="https://list.orgmode.org/tencent_04CF842704737012CCBCD63CD654DD41CA0A@qq.com/T/#m6ef8e7d34b25fe17b4cb655b161edce18c6655e">https://list.orgmode.org/tencent_04CF842704737012CCBCD63CD654DD41CA0A@qq.com/T/#m6ef8e7d34b25fe17b4cb655b161edce18c6655e,</a> <a href="https://git.savannah.gnu.org/cgiit/emacs/org-mode.git/commit/?id=8f8ec2ccf3f5ef8f38d">https://git.savannah.gnu.org/cgiit/emacs/org-mode.git/commit/?id=8f8ec2ccf3f5ef8f38d</a>	A-GNU-ORG-050423/687

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
				68ec84a7e 4739c45db 485	
<b>Vendor: go-huge-util_project</b>					
<b>Product: go-huge-util</b>					
Affected Version(s): * Up to (excluding) 0.0.34					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Mar-2023	8.8	go-used-util has commonly used utility functions for Go. Versions prior to 0.0.34 have a ZipSlip issue when using fsutil package to unzip files. When users use `zip.Unzip` to unzip zip files from a malicious attacker, they may be vulnerable to path traversal. The issue has been fixed in version 0.0.34. There are no known workarounds.  <b>CVE ID : CVE-2023-28105</b>	<a href="https://github.com/dablelv/go-huge-util/commit/0e308b0fac8973e6fa251b0ab095cdc5c1c0956b">https://github.com/dablelv/go-huge-util/commit/0e308b0fac8973e6fa251b0ab095cdc5c1c0956b</a>	A-GO--GO-H-050423/688
<b>Vendor: Google</b>					
<b>Product: chrome</b>					
Affected Version(s): * Up to (excluding) 111.0.5563.110					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-Mar-2023	9.8	Out of bounds memory access in WebHID in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a malicious HID device. (Chromium security severity: High)	<a href="https://chromerelease.s.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html">https://chromerelease.s.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html</a>	A-GOO-CHRO-050423/689

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
			<b>CVE ID : CVE-2023-1529</b>		
Use After Free	21-Mar-2023	8.8	Use after free in Passwords in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) <b>CVE ID : CVE-2023-1528</b>	<a href="https://chromerelease.s.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html">https://chromerelease.s.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html</a>	A-GOO-CHRO-050423/690
Use After Free	21-Mar-2023	8.8	Use after free in PDF in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) <b>CVE ID : CVE-2023-1530</b>	<a href="https://chromerelease.s.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html">https://chromerelease.s.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html</a>	A-GOO-CHRO-050423/691
Use After Free	21-Mar-2023	8.8	Use after free in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	<a href="https://chromerelease.s.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html">https://chromerelease.s.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html</a>	A-GOO-CHRO-050423/692

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
			<b>CVE ID : CVE-2023-1531</b>		
Out-of-bounds Read	21-Mar-2023	8.8	Out of bounds read in GPU Video in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) <b>CVE ID : CVE-2023-1532</b>	<a href="https://chromerelease.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html">https://chromerelease.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html</a>	A-GOO-CHRO-050423/693
Use After Free	21-Mar-2023	8.8	Use after free in WebProtect in Google Chrome prior to 111.0.5563.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) <b>CVE ID : CVE-2023-1533</b>	<a href="https://chromerelease.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html">https://chromerelease.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html</a>	A-GOO-CHRO-050423/694
Use After Free	21-Mar-2023	8.8	Out of bounds read in ANGLE in Google Chrome prior to 111.0.5563.110 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	<a href="https://chromerelease.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html">https://chromerelease.googleblog.com/2023/03/stable-channel-update-for-desktop_21.html</a>	A-GOO-CHRO-050423/695

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
			<b>CVE ID : CVE-2023-1534</b>		
<b>Product: tensorflow</b>					
Affected Version(s): * Up to (excluding) 2.12.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	25-Mar-2023	9.8	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, there is a heap buffer overflow in TAvPoolGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1. <b>CVE ID : CVE-2023-25664</b>	<a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-6hg6-5c2q-7rcr">https://github.com/tensorflow/tensorflow/security/advisories/GHSA-6hg6-5c2q-7rcr</a> , <a href="https://github.com/tensorflow/tensorflow/commit/ddaac2bdd099bec5d7923dea45276a7558217e5b">https://github.com/tensorflow/tensorflow/commit/ddaac2bdd099bec5d7923dea45276a7558217e5b</a>	A-GOO-TENS-050423/696
Out-of-bounds Read	25-Mar-2023	9.8	TensorFlow is an open source platform for machine learning. Attackers using Tensorflow prior to 2.12.0 or 2.11.1 can access heap memory which is not in the control of user, leading to a crash or remote code execution. The fix will be included in TensorFlow version 2.12.0 and will also cherry-pick this commit on TensorFlow version 2.11.1.	<a href="https://github.com/tensorflow/tensorflow/commit/7b174a0f2e40ff3f3aa957aecddfd5a7ae35ecb">https://github.com/tensorflow/tensorflow/commit/7b174a0f2e40ff3f3aa957aecddfd5a7ae35ecb</a> , <a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gw97-ff7c-9v96">https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gw97-ff7c-9v96</a>	A-GOO-TENS-050423/697

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
			<b>CVE ID : CVE-2023-25668</b>		
Out-of-bounds Read	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, an out of bounds read is in GRUBlockCellGrad. A fix is included in TensorFlow 2.12.0 and 2.11.1. <b>CVE ID : CVE-2023-25658</b>	<a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-68v3-g9cm-rmm6">https://github.com/tensorflow/tensorflow/security/advisories/GHSA-68v3-g9cm-rmm6</a> , <a href="https://github.com/tensorflow/tensorflow/commit/ff459137c2716a2a60f7d441b855fcb466d778cb">https://github.com/tensorflow/tensorflow/commit/ff459137c2716a2a60f7d441b855fcb466d778cb</a>	A-GOO-TENS-050423/698
Out-of-bounds Read	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, if the parameter `indices` for `DynamicStitch` does not match the shape of the parameter `data`, it can trigger an stack OOB read. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. <b>CVE ID : CVE-2023-25659</b>	<a href="https://github.com/tensorflow/tensorflow/commit/ee004b18b976eeb5a758020af8880236cd707d05">https://github.com/tensorflow/tensorflow/commit/ee004b18b976eeb5a758020af8880236cd707d05</a> , <a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-93vr-9q9m-pj8p">https://github.com/tensorflow/tensorflow/security/advisories/GHSA-93vr-9q9m-pj8p</a>	A-GOO-TENS-050423/699
NULL Pointer	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions	<a href="https://github.com/tensorflow/tensorflow/">https://github.com/tensorflow/</a>	A-GOO-TENS-050423/700

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
Dereference			2.12.0 and 2.11.1, when the parameter `summarize` of `tf.raw_ops.Print` is zero, the new method `SummarizeArray<bool>` will reference to a nullptr, leading to a seg fault. A fix is included in TensorFlow version 2.12 and version 2.11.1. <b>CVE ID : CVE-2023-25660</b>	commit/6d423b8bcc9aa9f5554dc988c1c16d038b508df1, <a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-qjqc-vqcf-5qvj">https://github.com/tensorflow/tensorflow/security/advisories/GHSA-qjqc-vqcf-5qvj</a>	
Integer Overflow or Wraparound	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Versions prior to 2.12.0 and 2.11.1 are vulnerable to integer overflow in EditDistance. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. <b>CVE ID : CVE-2023-25662</b>	<a href="https://github.com/tensorflow/tensorflow/commit/08b8e18643d6dcde00890733b270ff8d9960c56c">https://github.com/tensorflow/tensorflow/commit/08b8e18643d6dcde00890733b270ff8d9960c56c</a> , <a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-7jvm-xxmr-v5cw">https://github.com/tensorflow/tensorflow/security/advisories/GHSA-7jvm-xxmr-v5cw</a>	A-GOO-TENS-050423/701
NULL Pointer Dereference	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, when `ctx->step_containter()` is a null ptr, the Lookup function will be executed with a null	<a href="https://github.com/tensorflow/tensorflow/commit/239139d2ae6a81ae9ba499ad78b56d9b2931538a">https://github.com/tensorflow/tensorflow/commit/239139d2ae6a81ae9ba499ad78b56d9b2931538a</a> ,	A-GOO-TENS-050423/702

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
			pointer. A fix is included in TensorFlow 2.12.0 and 2.11.1. <b>CVE ID : CVE-2023-25663</b>	<a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-64jg-wjww-7c5w">https://github.com/tensorflow/tensorflow/security/advisories/GHSA-64jg-wjww-7c5w</a>	
NULL Pointer Dereference	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, when `SparseSparseMaximum` is given invalid sparse tensors as inputs, it can give a null pointer error. A fix is included in TensorFlow version 2.12 and version 2.11.1. <b>CVE ID : CVE-2023-25665</b>	<a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-558h-mq8x-7q9g">https://github.com/tensorflow/tensorflow/security/advisories/GHSA-558h-mq8x-7q9g</a> , <a href="https://github.com/tensorflow/tensorflow/commit/5e0ecfb42f5f65629fd7a4edd6c4afe7ff0feb04">https://github.com/tensorflow/tensorflow/commit/5e0ecfb42f5f65629fd7a4edd6c4afe7ff0feb04</a>	A-GOO-TENS-050423/703
Incorrect Comparison	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, there is a floating point exception in AudioSpectrogram. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. <b>CVE ID : CVE-2023-25666</b>	<a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f637-vh3r-vfh2">https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f637-vh3r-vfh2</a> , <a href="https://github.com/tensorflow/tensorflow/commit/d0d4e779da0d0f56499c6fa5ba09f0">https://github.com/tensorflow/tensorflow/commit/d0d4e779da0d0f56499c6fa5ba09f0</a>	A-GOO-TENS-050423/704

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
				a576cc6b14	
Integer Overflow or Wraparound	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, integer overflow occurs when $2^{31} \leq \text{num\_frames} * \text{height} * \text{width} * \text{channels} < 2^{32}$ , for example Full HD screencast of at least 346 frames. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. <b>CVE ID : CVE-2023-25667</b>	<a href="https://github.com/tensorflow/tensorflow/commit/8dc723fcdd1a6127d6c970bd2ecb18b019a1a58d">https://github.com/tensorflow/tensorflow/commit/8dc723fcdd1a6127d6c970bd2ecb18b019a1a58d</a> , <a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fqm2-gh8w-gr68">https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fqm2-gh8w-gr68</a>	A-GOO-TENS-050423/705
Incorrect Comparison	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Prior to versions 2.12.0 and 2.11.1, if the stride and window size are not positive for <code>`tf.raw_ops.AvgPoolGrad`</code> , it can give a floating point exception. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. <b>CVE ID : CVE-2023-25669</b>	<a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rcf8-g8jv-vg6p">https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rcf8-g8jv-vg6p</a> , <a href="https://github.com/tensorflow/tensorflow/commit/1295ae4dbb52fe06b19733b0257e2340d7b63b8d">https://github.com/tensorflow/tensorflow/commit/1295ae4dbb52fe06b19733b0257e2340d7b63b8d</a>	A-GOO-TENS-050423/706
NULL Pointer Dereference	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Versions prior to	<a href="https://github.com/tensorflow/tensorflow/">https://github.com/tensorflow/</a>	A-GOO-TENS-050423/707

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
			2.12.0 and 2.11.1 have a null point error in QuantizedMatMulWithBiasAndDequantize with MKL enabled. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. <b>CVE ID : CVE-2023-25670</b>	commit/8a47a39d9697969206d23a523c977238717e8727, <a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-49rq-hwc3-x77w">https://github.com/tensorflow/tensorflow/security/advisories/GHSA-49rq-hwc3-x77w</a>	
Out-of-bounds Write	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. There is out-of-bounds access due to mismatched integer type sizes. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. <b>CVE ID : CVE-2023-25671</b>	<a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-j5w9-hmfh-4cr6">https://github.com/tensorflow/tensorflow/security/advisories/GHSA-j5w9-hmfh-4cr6</a> , <a href="https://github.com/tensorflow/tensorflow/commit/2eedc8f676d2c3b8be9492e547b2bc814c10b367">https://github.com/tensorflow/tensorflow/commit/2eedc8f676d2c3b8be9492e547b2bc814c10b367</a>	A-GOO-TENS-050423/708
NULL Pointer Dereference	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. The function `tf.raw_ops.LookupTableImportV2` cannot handle scalars in the `values` parameter and gives an NPE. A fix is included in TensorFlow version	<a href="https://github.com/tensorflow/tensorflow/commit/980b22536abcbe1b4a5642fc940af33d8c19b69">https://github.com/tensorflow/tensorflow/commit/980b22536abcbe1b4a5642fc940af33d8c19b69</a> , <a href="https://git">https://git</a>	A-GOO-TENS-050423/709

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
			2.12.0 and version 2.11.1. <b>CVE ID : CVE-2023-25672</b>	hub.com/tensorflow/tensorflow/security/advisories/GHSA-94mm-g2mv-8p7r	
Incorrect Comparison	25-Mar-2023	7.5	TensorFlow is an open source platform for machine learning. Versions prior to 2.12.0 and 2.11.1 have a Floating Point Exception in TensorListSplit with XLA. A fix is included in TensorFlow version 2.12.0 and version 2.11.1. <b>CVE ID : CVE-2023-25673</b>	https://github.com/tensorflow/tensorflow/commit/728113a3be690facad6ce436660abc1858017fa, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-647v-r7qq-24fh	A-GOO-TENS-050423/710
NULL Pointer Dereference	25-Mar-2023	7.5	TensorFlow is an open source machine learning platform. Versions prior to 2.12.0 and 2.11.1 have a null pointer error in RandomShuffle with XLA enabled. A fix is included in TensorFlow 2.12.0 and 2.11.1. <b>CVE ID : CVE-2023-25674</b>	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-gf97-q72m-7579, https://github.com/tensorflow/tensorflow/commit/728113a3be690facad6ce436660a0b	A-GOO-TENS-050423/711

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
				c1858017fa	
Incorrect Comparison	25-Mar-2023	7.5	<p>TensorFlow is an end-to-end open source platform for machine learning. Constructing a tflite model with a parameter `filter_input_channel` of less than 1 gives a FPE. This issue has been patched in version 2.12. TensorFlow will also cherry-pick the fix commit on TensorFlow 2.11.1.</p> <p><b>CVE ID : CVE-2023-27579</b></p>	<p><a href="https://github.com/tensorflow/tensorflow/commit/34f8368c535253f5c9cb3a303297743b62442aa">https://github.com/tensorflow/tensorflow/commit/34f8368c535253f5c9cb3a303297743b62442aa</a>,  <a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-5w96-866f-6rm8">https://github.com/tensorflow/tensorflow/security/advisories/GHSA-5w96-866f-6rm8</a></p>	A-GOO-TENS-050423/712
<b>Vendor: gotowp</b>					
<b>Product: gotowp</b>					
Affected Version(s): * Up to (including) 5.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	<p>The GoToWP WordPress plugin through 5.1.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.</p> <p><b>CVE ID : CVE-2023-0369</b></p>	N/A	A-GOT-GOTO-050423/713
<b>Vendor: gpac</b>					

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
<b>Product: gpac</b>					
Affected Version(s): * Up to (including) 2.2.0					
Uncontrolled Resource Consumption	27-Mar-2023	7.8	Denial of Service in GitHub repository gpac/gpac prior to 2.4.0. <b>CVE ID : CVE-2023-1654</b>	<a href="https://huntr.dev/boonties/33652b56-128f-41a7-afcc-10641f69ff14">https://huntr.dev/boonties/33652b56-128f-41a7-afcc-10641f69ff14</a> , <a href="https://github.com/gpac/gpac/commit/2c055153d401b8c49422971e3a0159869652d3da">https://github.com/gpac/gpac/commit/2c055153d401b8c49422971e3a0159869652d3da</a>	A-GPA-GPAC-050423/714
Affected Version(s): 2.3					
Heap-based Buffer Overflow	17-Mar-2023	7.8	A vulnerability, which was classified as problematic, was found in GPAC 2.3-DEV-rev35-gbbca86917-master. This affects the function gf_m2ts_process_sdt of the file media_tools/mpegts.c. The manipulation leads to heap-based buffer overflow. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The identifier VDB-223293	N/A	A-GPA-GPAC-050423/715

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
			was assigned to this vulnerability. <b>CVE ID : CVE-2023-1448</b>		
Double Free	17-Mar-2023	7.8	A vulnerability has been found in GPAC 2.3-DEV-rev35-gbbca86917-master and classified as problematic. This vulnerability affects the function gf_av1_reset_state of the file media_tools/av_parsers.c. The manipulation leads to double free. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. VDB-223294 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1449</b>	<a href="https://github.com/gpac/gpac/issues/2387">https://github.com/gpac/gpac/issues/2387</a>	A-GPA-GPAC-050423/716
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Mar-2023	7.8	A vulnerability was found in GPAC 2.3-DEV-rev35-gbbca86917-master. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file filters/load_text.c. The manipulation leads to buffer overflow. Local	N/A	A-GPA-GPAC-050423/717

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
			<p>access is required to approach this attack. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The identifier VDB-223297 was assigned to this vulnerability.</p> <p><b>CVE ID : CVE-2023-1452</b></p>		
<b>Vendor: grafana</b>					
<b>Product: grafana</b>					
Affected Version(s): From (excluding) 9.3.0 Up to (excluding) 9.3.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	<p>Grafana is an open-source platform for monitoring and observability. Grafana had a stored XSS vulnerability in the Graphite FunctionDescription tooltip. The stored XSS vulnerability was possible due the value of the Function Description was not properly sanitized. An attacker needs to have control over the Graphite data source in order to manipulate a function description and a Grafana admin needs to configure the data source, later a Grafana user needs to select a tampered function and hover over the description.</p>	<p><a href="https://github.com/grafana/bugbounty/security/advisories/GHSA-qrrg-gw7w-vp76">https://github.com/grafana/bugbounty/security/advisories/GHSA-qrrg-gw7w-vp76</a>,  <a href="https://grafana.com/security/advisories/cve-2023-1410/">https://grafana.com/security/advisories/cve-2023-1410/</a></p>	A-GRA-GRAF-050423/718

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
			Users may upgrade to version 8.5.22, 9.2.15 and 9.3.11 to receive a fix. <b>CVE ID : CVE-2023-1410</b>		
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.5.22					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	Grafana is an open-source platform for monitoring and observability. Grafana had a stored XSS vulnerability in the Graphite FunctionDescription tooltip. The stored XSS vulnerability was possible due the value of the Function Description was not properly sanitized. An attacker needs to have control over the Graphite data source in order to manipulate a function description and a Grafana admin needs to configure the data source, later a Grafana user needs to select a tampered function and hover over the description. Users may upgrade to version 8.5.22, 9.2.15 and 9.3.11 to receive a fix. <b>CVE ID : CVE-2023-1410</b>	<a href="https://github.com/grafana/bugbounty/security/advisories/GHSA-qrrg-gw7w-7p76">https://github.com/grafana/bugbounty/security/advisories/GHSA-qrrg-gw7w-7p76</a> , <a href="https://grafana.com/security/security-advisories/cve-2023-1410/">https://grafana.com/security/security-advisories/cve-2023-1410/</a>	A-GRA-GRAF-050423/719
Affected Version(s): From (including) 9.2.0 Up to (excluding) 9.2.15					
Improper Neutralization	23-Mar-2023	4.8	Grafana is an open-source platform for	<a href="https://github.com/grafana/bugbounty/security/advisories/GHSA-qrrg-gw7w-7p76">https://github.com/grafana/bugbounty/security/advisories/GHSA-qrrg-gw7w-7p76</a>	A-GRA-GRAF-050423/720

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			<p>monitoring and observability. Grafana had a stored XSS vulnerability in the Graphite FunctionDescription tooltip. The stored XSS vulnerability was possible due the value of the Function Description was not properly sanitized. An attacker needs to have control over the Graphite data source in order to manipulate a function description and a Grafana admin needs to configure the data source, later a Grafana user needs to select a tampered function and hover over the description. Users may upgrade to version 8.5.22, 9.2.15 and 9.3.11 to receive a fix.</p> <p><b>CVE ID : CVE-2023-1410</b></p>	afana/bugbounty/security/advisories/GHSA-qrrg-gw7w-vp76, <a href="https://grafana.com/security/security-advisories/cve-2023-1410/">https://grafana.com/security/security-advisories/cve-2023-1410/</a>	

**Vendor: greenshiftwp**

**Product: greenshift\_ - animation\_and\_page\_builder\_blocks**

Affected Version(s): \* Up to (including) 4.9.9

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	<p>Auth. (author+) Cross-Site Scripting (XSS) vulnerability in Wpsoul Greenshift – animation and page builder blocks plugin &lt;= 4.9.9 versions.</p> <p><b>CVE ID : CVE-2023-22707</b></p>	N/A	A-GRE-GREE-050423/721
--	-------------	-----	---	-----	-----------------------

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
<b>Vendor: hasthemes</b>					
<b>Product: contact_form_7_widget_for_elementor_page_builder_&amp;_gutenberg_blocks</b>					
Affected Version(s): * Up to (excluding) 1.1.6					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The Contact Form 7 Widget For Elementor Page Builder & Gutenberg Blocks WordPress plugin before 1.1.6 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack <b>CVE ID : CVE-2023-0484</b>	N/A	A-HAS-CONT-050423/722
<b>Product: coupon_zen</b>					
Affected Version(s): * Up to (excluding) 1.0.6					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The Coupon Zen WordPress plugin before 1.0.6 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack <b>CVE ID : CVE-2023-1089</b>	N/A	A-HAS-COUP-050423/723
<b>Product: ever_compare</b>					
Affected Version(s): * Up to (including) 1.2.3					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The Ever Compare WordPress plugin through 1.2.3 does not have CSRF check when	N/A	A-HAS-EVER-050423/724

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
			activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack <b>CVE ID : CVE-2023-0505</b>		
<b>Product: free_woocommerce_theme_99fy_extension</b>					
Affected Version(s): * Up to (excluding) 1.2.8					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The Free WooCommerce Theme 99fy Extension WordPress plugin before 1.2.8 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack <b>CVE ID : CVE-2023-0503</b>	N/A	A-HAS-FREE-050423/725
<b>Product: ht_event</b>					
Affected Version(s): * Up to (excluding) 1.4.6					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The HT Event WordPress plugin before 1.4.6 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack <b>CVE ID : CVE-2023-0496</b>	N/A	A-HAS-HT_E-050423/726

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
<b>Product: ht_politic</b>					
Affected Version(s): * Up to (excluding) 2.3.8					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The HT Politic WordPress plugin before 2.3.8 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack <b>CVE ID : CVE-2023-0504</b>	N/A	A-HAS-HT_P-050423/727
<b>Product: ht_portfolio</b>					
Affected Version(s): * Up to (excluding) 1.1.6					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The HT Portfolio WordPress plugin before 1.1.6 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack <b>CVE ID : CVE-2023-0497</b>	N/A	A-HAS-HT_P-050423/728
<b>Product: ht_slider_for_elementor</b>					
Affected Version(s): * Up to (excluding) 1.4.0					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The HT Slider For Elementor WordPress plugin before 1.4.0 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate	N/A	A-HAS-HT_S-050423/729

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
			arbitrary plugins present on the blog via a CSRF attack <b>CVE ID : CVE-2023-0495</b>		
<b>Product: preview_link_generator</b>					
Affected Version(s): * Up to (excluding) 1.0.4					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The Preview Link Generator WordPress plugin before 1.0.4 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack <b>CVE ID : CVE-2023-1086</b>	N/A	A-HAS-PREV-050423/730
<b>Product: quickswish</b>					
Affected Version(s): * Up to (excluding) 1.1.0					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The QuickSwish WordPress plugin before 1.1.0 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack <b>CVE ID : CVE-2023-0499</b>	N/A	A-HAS-QUIC-050423/731
<b>Product: wc_sales_notification</b>					
Affected Version(s): * Up to (excluding) 1.2.3					
Cross-Site Request	27-Mar-2023	4.3	The WC Sales Notification	N/A	A-HAS-WC_S-050423/732

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
Forgery (CSRF)			WordPress plugin before 1.2.3 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack <b>CVE ID : CVE-2023-1087</b>		
<b>Product: wp_education</b>					
Affected Version(s): * Up to (excluding) 1.2.7					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The WP Education WordPress plugin before 1.2.7 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack <b>CVE ID : CVE-2023-0498</b>	N/A	A-HAS-WP_E-050423/733
<b>Product: wp_film_studio</b>					
Affected Version(s): * Up to (excluding) 1.3.5					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	6.5	The WP Film Studio WordPress plugin before 1.3.5 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack	N/A	A-HAS-WP_F-050423/734

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-0500</b>		
<b>Product: wp_insurance</b>					
Affected Version(s): * Up to (excluding) 2.1.4					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	6.5	The WP Insurance WordPress plugin before 2.1.4 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack <b>CVE ID : CVE-2023-0501</b>	N/A	A-HAS-WP_I-050423/735
<b>Product: wp_news</b>					
Affected Version(s): * Up to (including) 1.1.9					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	6.5	The WP News WordPress plugin through 1.1.9 does not have CSRF check when activating plugins, which could allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack <b>CVE ID : CVE-2023-0502</b>	N/A	A-HAS-WP_N-050423/736
<b>Product: wp_plugin_manager</b>					
Affected Version(s): * Up to (excluding) 1.1.8					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	4.3	The WP Plugin Manager WordPress plugin before 1.1.8 does not have CSRF check when activating plugins, which could	N/A	A-HAS-WP_P-050423/737

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
			allow attackers to make logged in admins activate arbitrary plugins present on the blog via a CSRF attack  <b>CVE ID : CVE-2023-1088</b>		
<b>Vendor: hgiga</b>					
<b>Product: oaklouds_mailsherlock</b>					
Affected Version(s): 4.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Mar-2023	7.2	HGiga MailSherlock mail query function has vulnerability of insufficient validation for user input. An authenticated remote attacker with administrator privilege can exploit this vulnerability to inject SQL commands to read, modify, and delete the database.  <b>CVE ID : CVE-2023-24840</b>	<a href="https://www.twcert.org.tw/tw/cp-132-6959-cdecb-1.html">https://www.twcert.org.tw/tw/cp-132-6959-cdecb-1.html</a>	A-HGI-OAKL-050423/738
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Mar-2023	7.2	HGiga MailSherlock query function for connection log has a vulnerability of insufficient filtering for user input. An authenticated remote attacker with administrator privilege can exploit this vulnerability to inject and execute arbitrary system commands to perform arbitrary system	<a href="https://www.twcert.org.tw/tw/cp-132-6960-fc2fe-1.html">https://www.twcert.org.tw/tw/cp-132-6960-fc2fe-1.html</a>	A-HGI-OAKL-050423/739

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
			operation or disrupt service. <b>CVE ID : CVE-2023-24841</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	HGiga MailSherlock's specific function has insufficient filtering for user input. An unauthenticated remote attacker can exploit this vulnerability to inject JavaScript, conducting a reflected XSS attack. <b>CVE ID : CVE-2023-24839</b>	<a href="https://www.twcert.org.tw/tw/cp-132-6958-e1a8e-1.html">https://www.twcert.org.tw/tw/cp-132-6958-e1a8e-1.html</a>	A-HGI-OAKL-050423/740
Authorization Bypass Through User-Controlled Key	27-Mar-2023	5.3	HGiga MailSherlock has vulnerability of insufficient access control. An unauthenticated remote user can exploit this vulnerability to access partial content of another user's mail by changing user ID and mail ID within URL. <b>CVE ID : CVE-2023-24842</b>	<a href="https://www.twcert.org.tw/tw/cp-132-6961-12444-1.html">https://www.twcert.org.tw/tw/cp-132-6961-12444-1.html</a>	A-HGI-OAKL-050423/741
<b>Product: oakclouds_portal</b>					
Affected Version(s): From (including) 2.0 Up to (excluding) 2.0-10					
Unrestricted Upload of File with Dangerous Type	27-Mar-2023	9.8	HGiga OAKclouds file uploading function does not restrict upload of file with dangerous type. An unauthenticated remote attacker can exploit this vulnerability to	<a href="https://www.twcert.org.tw/tw/cp-132-6973-45872-1.html">https://www.twcert.org.tw/tw/cp-132-6973-45872-1.html</a>	A-HGI-OAKL-050423/742

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upload and run arbitrary executable files to perform arbitrary command or disrupt service. <b>CVE ID : CVE-2023-25909</b>		
Affected Version(s): From (including) 3.0 Up to (excluding) 3.0-10					
Unrestricted Upload of File with Dangerous Type	27-Mar-2023	9.8	HGiga OAKclouds file uploading function does not restrict upload of file with dangerous type. An unauthenticated remote attacker can exploit this vulnerability to upload and run arbitrary executable files to perform arbitrary command or disrupt service. <b>CVE ID : CVE-2023-25909</b>	<a href="https://www.twcert.org.tw/tw/cp-132-6973-45872-1.html">https://www.twcert.org.tw/tw/cp-132-6973-45872-1.html</a>	A-HGI-OAKL-050423/743
<b>Vendor: hkcms_project</b>					
<b>Product: hkcms</b>					
Affected Version(s): 2.2.4.230206					
Improper Control of Generation of Code ('Code Injection')	18-Mar-2023	8.8	A vulnerability, which was classified as problematic, was found in HkCms 2.2.4.230206. This affects an unknown part of the file /admin.php/appcenter/local.html?type=addon of the component External Plugin Handler. The manipulation leads to code injection. It is	N/A	A-HKC-HKCM-050423/744

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
			possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223365 was assigned to this vulnerability. <b>CVE ID : CVE-2023-1482</b>		
<b>Vendor: hu-manity</b>					
<b>Product: cookie_notice_\&amp;_compliance_for_gdpr_\/_ccpa</b>					
Affected Version(s): * Up to (excluding) 2.4.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	The Cookie Notice & Compliance for GDPR / CCPA WordPress plugin before 2.4.7 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks <b>CVE ID : CVE-2023-0823</b>	N/A	A-HU--COOK-050423/745
<b>Vendor: IBM</b>					
<b>Product: aspera_faspex</b>					
Affected Version(s): * Up to (including) 4.4.2					
Improper Restriction of XML External	21-Mar-2023	8.8	IBM Aspera Faspex 4.4.2 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote	<a href="https://www.ibm.com/support/pages/node/6964694">https://www.ibm.com/support/pages/node/6964694</a> , <a href="https://exc">https://exc</a>	A-IBM-ASPE-050423/746

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
Entity Reference			authenticated attacker could exploit this vulnerability to execute arbitrary commands. IBM X-Force ID: 249845. <b>CVE ID : CVE-2023-27874</b>	hange.xforce.ibmcloud.com/vulnerabilities/249845	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	7.5	IBM Aspera Faspex 4.4.2 could allow a remote attacker to obtain sensitive credential information for an external user, using a specially crafted SQL query. IBM X-Force ID: 249613. <b>CVE ID : CVE-2023-27871</b>	<a href="https://www.ibm.com/support/pages/node/6964694">https://www.ibm.com/support/pages/node/6964694</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/249613">https://exchange.xforce.ibmcloud.com/vulnerabilities/249613</a>	A-IBM-ASPE-050423/747
N/A	21-Mar-2023	6.5	IBM Aspera Faspex 4.4.2 could allow a remote authenticated attacker to obtain sensitive credential information using specially crafted XML input. IBM X-Force ID: 249654. <b>CVE ID : CVE-2023-27873</b>	<a href="https://www.ibm.com/support/pages/node/6964694">https://www.ibm.com/support/pages/node/6964694</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/249654">https://exchange.xforce.ibmcloud.com/vulnerabilities/249654</a>	A-IBM-ASPE-050423/748
Affected Version(s): 4.4.2					
Improper Restriction of XML External Entity Reference	21-Mar-2023	8.8	IBM Aspera Faspex 4.4.2 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote authenticated attacker could exploit this vulnerability to execute arbitrary	<a href="https://www.ibm.com/support/pages/node/6964694">https://www.ibm.com/support/pages/node/6964694</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/249654">https://exchange.xforce.ibmcloud.com/vulnerabilities/249654</a>	A-IBM-ASPE-050423/749

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
			commands. IBM X-Force ID: 249845. <b>CVE ID : CVE-2023-27874</b>	abilities/249845	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	7.5	IBM Aspera Faspex 4.4.2 could allow a remote attacker to obtain sensitive credential information for an external user, using a specially crafted SQL query. IBM X-Force ID: 249613. <b>CVE ID : CVE-2023-27871</b>	<a href="https://www.ibm.com/support/pages/node/6964694">https://www.ibm.com/support/pages/node/6964694</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/249613">https://exchange.xforce.ibmcloud.com/vulnerabilities/249613</a>	A-IBM-ASPE-050423/750
N/A	21-Mar-2023	6.5	IBM Aspera Faspex 4.4.2 could allow a remote authenticated attacker to obtain sensitive credential information using specially crafted XML input. IBM X-Force ID: 249654. <b>CVE ID : CVE-2023-27873</b>	<a href="https://www.ibm.com/support/pages/node/6964694">https://www.ibm.com/support/pages/node/6964694</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/249654">https://exchange.xforce.ibmcloud.com/vulnerabilities/249654</a>	A-IBM-ASPE-050423/751
Affected Version(s): 5.0.4					
N/A	16-Mar-2023	7.5	IBM Aspera Faspex 5.0.4 could allow a user to change other user's credentials due to improper access controls. IBM X-Force ID: 249847. <b>CVE ID : CVE-2023-27875</b>	<a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/249847">https://exchange.xforce.ibmcloud.com/vulnerabilities/249847</a> , <a href="https://www.ibm.com/support/pages/node/6963662">https://www.ibm.com/support/pages/node/6963662</a>	A-IBM-ASPE-050423/752
<b>Product: security_key_lifecycle_manager</b>					
Affected Version(s): 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 Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	9.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 247597. <b>CVE ID : CVE-2023-25684</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247597">https://exchange.xforce.ibmcloud.com/vulnerabilities/247597</a>	A-IBM-SECU-050423/753
Incorrect Authorization	22-Mar-2023	8.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to perform actions that they should not have access to due to improper authorization. IBM X-Force ID: 247630. <b>CVE ID : CVE-2023-25924</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247630">https://exchange.xforce.ibmcloud.com/vulnerabilities/247630</a>	A-IBM-SECU-050423/754
Incorrect Authorization	21-Mar-2023	7.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an attacker to upload files that could be used in a denial of service attack due to incorrect	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247597">https://exchange.xforce.ibmcloud.com/vulnerabilities/247597</a>	A-IBM-SECU-050423/755

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
			authorization. IBM X-Force ID: 247629. <b>CVE ID : CVE-2023-25923</b>	abilities/247629	
Insufficiently Protected Credentials	21-Mar-2023	5.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 247601. <b>CVE ID : CVE-2023-25686</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247601">https://exchange.xforce.ibmcloud.com/vulnerabilities/247601</a>	A-IBM-SECU-050423/756
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 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: 247606. <b>CVE ID : CVE-2023-25688</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247606">https://exchange.xforce.ibmcloud.com/vulnerabilities/247606</a>	A-IBM-SECU-050423/757
Improper Limitation of a Pathname to a Restricted Directory	21-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow a remote attacker to traverse directories on the system. An	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247606">https://exchange.xforce.ibmcloud.com/vulnerabilities/247606</a>	A-IBM-SECU-050423/758

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
('Path Traversal')			attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 247618. <b>CVE ID : CVE-2023-25689</b>	com/vulnerabilities/247618	
Insertion of Sensitive Information into Log File	21-Mar-2023	4.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to obtain sensitive information from log files. IBM X-Force ID: 247602. <b>CVE ID : CVE-2023-25687</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a>	A-IBM-SECU-050423/759
Affected Version(s): 3.0.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	9.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 247597. <b>CVE ID : CVE-2023-25684</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247597">https://exchange.xforce.ibmcloud.com/vulnerabilities/247597</a>	A-IBM-SECU-050423/760

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	22-Mar-2023	8.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to perform actions that they should not have access to due to improper authorization. IBM X-Force ID: 247630. <b>CVE ID : CVE-2023-25924</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247630">https://exchange.xforce.ibmcloud.com/vulnerabilities/247630</a>	A-IBM-SECU-050423/761
Incorrect Authorization	21-Mar-2023	7.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an attacker to upload files that could be used in a denial of service attack due to incorrect authorization. IBM X-Force ID: 247629. <b>CVE ID : CVE-2023-25923</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247629">https://exchange.xforce.ibmcloud.com/vulnerabilities/247629</a>	A-IBM-SECU-050423/762
Insufficiently Protected Credentials	21-Mar-2023	5.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 247601. <b>CVE ID : CVE-2023-25686</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247601">https://exchange.xforce.ibmcloud.com/vulnerabilities/247601</a>	A-IBM-SECU-050423/763
Improper Limitation	22-Mar-2023	5.3	IBM Security Guardium Key	<a href="https://www.ibm.com">https://www.ibm.com</a>	A-IBM-SECU-050423/764

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
of a Pathname to a Restricted Directory ('Path Traversal')			Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 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: 247606. <b>CVE ID : CVE-2023-25688</b>	/support/pages/node/6962729, <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247606">https://exchange.xforce.ibmcloud.com/vulnerabilities/247606</a>	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 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: 247618. <b>CVE ID : CVE-2023-25689</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247618">https://exchange.xforce.ibmcloud.com/vulnerabilities/247618</a>	A-IBM-SECU-050423/765
Insertion of Sensitive Information into Log File	21-Mar-2023	4.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to obtain sensitive information from log	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a>	A-IBM-SECU-050423/766

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
			files. IBM X-Force ID: 247602. <b>CVE ID : CVE-2023-25687</b>		
Affected Version(s): 4.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	9.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 247597. <b>CVE ID : CVE-2023-25684</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247597">https://exchange.xforce.ibmcloud.com/vulnerabilities/247597</a>	A-IBM-SECU-050423/767
Incorrect Authorization	22-Mar-2023	8.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to perform actions that they should not have access to due to improper authorization. IBM X-Force ID: 247630. <b>CVE ID : CVE-2023-25924</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247630">https://exchange.xforce.ibmcloud.com/vulnerabilities/247630</a>	A-IBM-SECU-050423/768
Incorrect Authorization	21-Mar-2023	7.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> ,	A-IBM-SECU-050423/769

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to upload files that could be used in a denial of service attack due to incorrect authorization. IBM X-Force ID: 247629. <b>CVE ID : CVE-2023-25923</b>	<a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247629">https://exchange.xforce.ibmcloud.com/vulnerabilities/247629</a>	
Insufficiently Protected Credentials	21-Mar-2023	5.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 247601. <b>CVE ID : CVE-2023-25686</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247601">https://exchange.xforce.ibmcloud.com/vulnerabilities/247601</a>	A-IBM-SECU-050423/770
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 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: 247606. <b>CVE ID : CVE-2023-25688</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247606">https://exchange.xforce.ibmcloud.com/vulnerabilities/247606</a>	A-IBM-SECU-050423/771
Improper Limitation of a	21-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0,	<a href="https://www.ibm.com/support/p">https://www.ibm.com/support/p</a>	A-IBM-SECU-050423/772

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			3.0.1, 4.0, 4.1 , and 4.1.1 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: 247618. <b>CVE ID : CVE-2023-25689</b>	ages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247618	
Insertion of Sensitive Information into Log File	21-Mar-2023	4.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to obtain sensitive information from log files. IBM X-Force ID: 247602. <b>CVE ID : CVE-2023-25687</b>	https://www.ibm.com/support/pages/node/6962729	A-IBM-SECU-050423/773
Affected Version(s): 4.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	9.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database.	https://www.ibm.com/support/pages/node/6962729, https://exchange.xforce.ibmcloud.com/vulnerabilities/247597	A-IBM-SECU-050423/774

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
			IBM X-Force ID: 247597. <b>CVE ID : CVE-2023-25684</b>		
Incorrect Authorization	22-Mar-2023	8.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to perform actions that they should not have access to due to improper authorization. IBM X-Force ID: 247630. <b>CVE ID : CVE-2023-25924</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247630">https://exchange.xforce.ibmcloud.com/vulnerabilities/247630</a>	A-IBM-SECU-050423/775
Incorrect Authorization	21-Mar-2023	7.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an attacker to upload files that could be used in a denial of service attack due to incorrect authorization. IBM X-Force ID: 247629. <b>CVE ID : CVE-2023-25923</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247629">https://exchange.xforce.ibmcloud.com/vulnerabilities/247629</a>	A-IBM-SECU-050423/776
Insufficiently Protected Credentials	21-Mar-2023	5.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 247601.	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247601">https://exchange.xforce.ibmcloud.com/vulnerabilities/247601</a>	A-IBM-SECU-050423/777

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
			<b>CVE ID : CVE-2023-25686</b>	abilities/247601	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 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: 247606. <b>CVE ID : CVE-2023-25688</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247606">https://exchange.xforce.ibmcloud.com/vulnerabilities/247606</a>	A-IBM-SECU-050423/778
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1 , and 4.1.1 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: 247618. <b>CVE ID : CVE-2023-25689</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247618">https://exchange.xforce.ibmcloud.com/vulnerabilities/247618</a>	A-IBM-SECU-050423/779
Insertion of Sensitive Informatio	21-Mar-2023	4.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and	<a href="https://www.ibm.com/support/p">https://www.ibm.com/support/p</a>	A-IBM-SECU-050423/780

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 into Log File			4.1.1 could allow an authenticated user to obtain sensitive information from log files. IBM X-Force ID: 247602. <b>CVE ID : CVE-2023-25687</b>	ages/node/6962729	
Affected Version(s): 4.1.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	9.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 247597. <b>CVE ID : CVE-2023-25684</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247597">https://exchange.xforce.ibmcloud.com/vulnerabilities/247597</a>	A-IBM-SECU-050423/781
Incorrect Authorization	22-Mar-2023	8.8	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to perform actions that they should not have access to due to improper authorization. IBM X-Force ID: 247630. <b>CVE ID : CVE-2023-25924</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247630">https://exchange.xforce.ibmcloud.com/vulnerabilities/247630</a>	A-IBM-SECU-050423/782

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	21-Mar-2023	7.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an attacker to upload files that could be used in a denial of service attack due to incorrect authorization. IBM X-Force ID: 247629. <b>CVE ID : CVE-2023-25923</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247629">https://exchange.xforce.ibmcloud.com/vulnerabilities/247629</a>	A-IBM-SECU-050423/783
Insufficiently Protected Credentials	21-Mar-2023	5.5	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 247601. <b>CVE ID : CVE-2023-25686</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247601">https://exchange.xforce.ibmcloud.com/vulnerabilities/247601</a>	A-IBM-SECU-050423/784
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 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: 247606.	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247606">https://exchange.xforce.ibmcloud.com/vulnerabilities/247606</a>	A-IBM-SECU-050423/785

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
			<b>CVE ID : CVE-2023-25688</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Mar-2023	5.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1 , and 4.1.1 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: 247618. <b>CVE ID : CVE-2023-25689</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/247618">https://exchange.xforce.ibmcloud.com/vulnerabilities/247618</a>	A-IBM-SECU-050423/786
Insertion of Sensitive Information into Log File	21-Mar-2023	4.3	IBM Security Guardium Key Lifecycle Manager 3.0, 3.0.1, 4.0, 4.1, and 4.1.1 could allow an authenticated user to obtain sensitive information from log files. IBM X-Force ID: 247602. <b>CVE ID : CVE-2023-25687</b>	<a href="https://www.ibm.com/support/pages/node/6962729">https://www.ibm.com/support/pages/node/6962729</a>	A-IBM-SECU-050423/787
<b>Vendor: ibos</b>					
<b>Product: ibos</b>					
Affected Version(s): 4.5.5					
Improper Neutralization of Special Elements used in an	18-Mar-2023	9.8	A vulnerability classified as critical has been found in IBOS 4.5.5. Affected is an unknown function of the file	N/A	A-IBO-IBOS-050423/788

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			<p>ApiController.php.</p> <p>The manipulation of the argument emailids 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-223380.</p> <p><b>CVE ID : CVE-2023-1494</b></p>		

**Vendor: Imagemagick**

**Product: imagemagick**

Affected Version(s): \* Up to (excluding) 7.1.1-0

Improper Input Validation	23-Mar-2023	5.5	<p>A vulnerability was discovered in ImageMagick where a specially created SVG file loads itself and causes a segmentation fault. This flaw allows a remote attacker to pass a specially crafted SVG file that leads to a segmentation fault, generating many trash files in "/tmp," resulting in a denial of service. When ImageMagick crashes, it generates a lot of trash files. These trash files can be large if the SVG file contains many render actions. In a denial of service attack, if a remote attacker uploads an</p>	<p><a href="https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4">https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4</a>,  <a href="https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr">https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr</a>,  <a href="https://bugzilla.redhat.com/show_bug.cgi?id=2176858">https://bugzilla.redhat.com/show_bug.cgi?id=2176858</a></p>	A-IMA-IMAG-050423/789
---------------------------	-------------	-----	---	--	-----------------------

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
			<p>SVG file of size t, ImageMagick generates files of size 103*t. If an attacker uploads a 100M SVG, the server will generate about 10G.</p> <p><b>CVE ID : CVE-2023-1289</b></p>		
<b>Vendor: implecode</b>					
<b>Product: ecommerce_product_catalog</b>					
Affected Version(s): * Up to (excluding) 3.3.9					
<p>Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')</p>	17-Mar-2023	4.8	<p>The eCommerce Product Catalog plugin for WordPress is vulnerable to Stored Cross-Site Scripting via some of its settings parameters in versions up to, and including, 3.3.8 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. This only affects multi-site installations and installations where unfiltered_html has been disabled.</p> <p><b>CVE ID : CVE-2023-1470</b></p>	<p><a href="https://plugins.trac.wordpress.org/changest/2881773/e-commerce-product-catalog/trunk/modules/price/price-settings.php">https://plugins.trac.wordpress.org/changest/2881773/e-commerce-product-catalog/trunk/modules/price/price-settings.php</a></p>	A-IMP-ECOM-050423/790

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
<b>Vendor: independentsoft</b>					
<b>Product: jodf</b>					
Affected Version(s): * Up to (excluding) 1.1.110					
Improper Restriction of XML External Entity Reference	24-Mar-2023	9.8	An issue was discovered in Independentsoft JODF before 1.1.110. The API is prone to XML external entity (XXE) injection via a remote DTD in a DOCX file. <b>CVE ID : CVE-2023-28150</b>	N/A	A-IND-JODF-050423/791
<b>Product: jspreadsheet</b>					
Affected Version(s): * Up to (excluding) 1.1.110					
Improper Restriction of XML External Entity Reference	24-Mar-2023	9.8	An issue was discovered in Independentsoft JSpreadsheet before 1.1.110. The API is prone to XML external entity (XXE) injection via a remote DTD in a DOCX file. <b>CVE ID : CVE-2023-28151</b>	N/A	A-IND-JSPR-050423/792
<b>Product: jword</b>					
Affected Version(s): * Up to (excluding) 1.1.110					
Improper Restriction of XML External Entity Reference	24-Mar-2023	9.8	An issue was discovered in Independentsoft JWord before 1.1.110. The API is prone to XML external entity (XXE) injection via a remote DTD in a DOCX file. <b>CVE ID : CVE-2023-28152</b>	N/A	A-IND-JWOR-050423/793

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
<b>Vendor: invernyx</b>					
<b>Product: smartcars_3</b>					
Affected Version(s): * Up to (excluding) 0.5.9					
Insertion of Sensitive Information into Log File	24-Mar-2023	7.5	smartCARS 3 is flight tracking software. In version 0.5.8 and prior, all persons who have failed login attempts will have their password stored in error logs. This problem doesn't occur in version 0.5.9. As a workaround, delete the affected log file, and ensure one logs in correctly.  <b>CVE ID : CVE-2023-28441</b>	<a href="https://github.com/invernyx/smartcars-3-bugs/security/advisories/GHSA-fp42-c8g2-5jc7">https://github.com/invernyx/smartcars-3-bugs/security/advisories/GHSA-fp42-c8g2-5jc7</a>	A-INV-SMAR-050423/794
<b>Vendor: Iobit</b>					
<b>Product: malware_fighter</b>					
Affected Version(s): 9.4.0.776					
Out-of-bounds Write	26-Mar-2023	7.8	A vulnerability was found in IObit Malware Fighter 9.4.0.776. It has been declared as critical. This vulnerability affects the function 0x8018E000/0x8018E004 in the library IMFCameraProtect.sys of the component IOCTL Handler. The manipulation leads to stack-based buffer overflow. An attack has to be approached locally. The exploit has been disclosed to the public and may be	N/A	A-IOB-MALW-050423/795

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. VDB-224026 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1646</b>		
Improper Resource Shutdown or Release	26-Mar-2023	5.5	A vulnerability was found in IObit Malware Fighter 9.4.0.776. It has been rated as problematic. Affected by this issue is the function 0x8001E024/0x8001E040 in the library ImRegistryFilter.sys of the component IOCTL Handler. The manipulation leads to denial of service. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. VDB-224018 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1638</b>	N/A	A-IOB-MALW-050423/796
Improper Resource Shutdown or Release	26-Mar-2023	5.5	A vulnerability classified as problematic has been found in IObit Malware Fighter 9.4.0.776. This affects the function 0x8001E04C in the library ImRegistryFilter.sys of the component IOCTL Handler. The manipulation leads to denial of service. It is	N/A	A-IOB-MALW-050423/797

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
			possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224019. <b>CVE ID : CVE-2023-1639</b>		
Improper Resource Shutdown or Release	26-Mar-2023	5.5	A vulnerability classified as problematic was found in IObit Malware Fighter 9.4.0.776. This vulnerability affects the function 0x222010 in the library ObCallbackProcess.sys of the component IOCTL Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224020. <b>CVE ID : CVE-2023-1640</b>	N/A	A-IOB-MALW-050423/798
Improper Resource Shutdown or Release	26-Mar-2023	5.5	A vulnerability, which was classified as problematic, has been found in IObit Malware Fighter 9.4.0.776. This issue affects the function	N/A	A-IOB-MALW-050423/799

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
			<p>0x222018 in the library ObCallbackProcess.sys of the component IOCTL Handler. The manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier VDB-224021 was assigned to this vulnerability.</p> <p><b>CVE ID : CVE-2023-1641</b></p>		
Improper Resource Shutdown or Release	26-Mar-2023	5.5	<p>A vulnerability, which was classified as problematic, was found in IObit Malware Fighter 9.4.0.776. Affected is the function 0x222034/0x222038/0x22203C/0x222040 in the library ObCallbackProcess.sys of the component IOCTL Handler. The manipulation leads to denial of service. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. VDB-224022 is the identifier assigned to this vulnerability.</p> <p><b>CVE ID : CVE-2023-1642</b></p>	N/A	A-IOB-MALW-050423/800

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 Resource Shutdown or Release	26-Mar-2023	5.5	<p>A vulnerability has been found in IObit Malware Fighter 9.4.0.776 and classified as problematic. Affected by this vulnerability is the function 0x8001E000/0x8001E004/0x8001E018/0x8001E01C/0x8001E024/0x8001E040 in the library ImfHpRegFilter.sys of the component IOCTL Handler. The manipulation leads to denial of service. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224023.</p> <p><b>CVE ID : CVE-2023-1643</b></p>	N/A	A-IOB-MALW-050423/801
Improper Resource Shutdown or Release	26-Mar-2023	5.5	<p>A vulnerability was found in IObit Malware Fighter 9.4.0.776 and classified as problematic. Affected by this issue is the function 0x8018E010 in the library IMFCameraProtect.sys of the component IOCTL Handler. The manipulation leads to denial of service. It is possible to launch the</p>	N/A	A-IOB-MALW-050423/802

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
			<p>attack on the local host. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224024.</p> <p><b>CVE ID : CVE-2023-1644</b></p>		
Improper Resource Shutdown or Release	26-Mar-2023	5.5	<p>A vulnerability was found in IObit Malware Fighter 9.4.0.776. It has been classified as problematic. This affects the function 0x8018E008 in the library IMFCameraProtect.sys of the component IOCTL Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier VDB-224025 was assigned to this vulnerability.</p> <p><b>CVE ID : CVE-2023-1645</b></p>	N/A	A-IOB-MALW-050423/803
<b>Vendor: isdecisions</b>					
<b>Product: userlock</b>					
Affected Version(s): 11.0.1					
Incorrect Authorization	23-Mar-2023	7.2	<p>IS Decisions UserLock MFA 11.01 is vulnerable to authentication bypass using scheduled task.</p>	N/A	A-ISD-USER-050423/804

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
			<b>CVE ID : CVE-2023-23192</b>		
<b>Vendor: jc21</b>					
<b>Product: nginx_proxy_manager</b>					
Affected Version(s): 2.9.19					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Mar-2023	9.8	An issue found in NginxProxyManager v.2.9.19 allows an attacker to execute arbitrary code via a lua script to the configuration file. <b>CVE ID : CVE-2023-27224</b>	N/A	A-JC2-NGIN-050423/805
<b>Vendor: jeecg</b>					
<b>Product: jeecg-boot</b>					
Affected Version(s): 3.5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability classified as critical has been found in jeecg-boot 3.5.0. This affects an unknown part of the file jmreport/questSql. The manipulation of the argument apiSelectId leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223299. <b>CVE ID : CVE-2023-1454</b>	N/A	A-JEE-JEEC-050423/806
<b>Vendor: Jenkins</b>					

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
<b>Product: absint_a3</b>					
Affected Version(s): * Up to (including) 1.1.0					
Improper Restriction of XML External Entity Reference	22-Mar-2023	7.1	Jenkins AbsInt a <sup>3</sup> Plugin 1.1.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. <b>CVE ID : CVE-2023-28685</b>	<a href="https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-2930">https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-2930</a>	A-JEN-ABSI-050423/807
<b>Vendor: jettison_project</b>					
<b>Product: jettison</b>					
Affected Version(s): * Up to (excluding) 1.5.4					
Uncontrolled Recursion	22-Mar-2023	7.5	An infinite recursion is triggered in Jettison when constructing a JSONArray from a Collection that contains a self-reference in one of its elements. This leads to a StackOverflowError exception being thrown. <b>CVE ID : CVE-2023-1436</b>	N/A	A-JET-JETT-050423/808
<b>Vendor: Jiangmin</b>					
<b>Product: jiangmin_antivirus</b>					
Affected Version(s): 16.2.2022.418					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-Mar-2023	7.8	A vulnerability classified as critical was found in JiangMin Antivirus 16.2.2022.418. Affected by this vulnerability is the function 0x222010 in the library kvcore.sys of the component	N/A	A-JIA-JIAN-050423/809

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
			IOCTL Handler. The manipulation leads to memory corruption. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224011. <b>CVE ID : CVE-2023-1629</b>		
NULL Pointer Dereference	25-Mar-2023	5.5	A vulnerability classified as problematic has been found in Jianming Antivirus 16.2.2022.418. Affected is an unknown function in the library kvcore.sys of the component IoControlCode Handler. The manipulation leads to null pointer dereference. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. VDB-224010 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1628</b>	N/A	A-JIA-JIAN-050423/810
Improper Resource Shutdown or Release	25-Mar-2023	5.5	A vulnerability, which was classified as problematic, has been found in JiangMin Antivirus	N/A	A-JIA-JIAN-050423/811

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
			<p>16.2.2022.418. Affected by this issue is the function 0x222000 in the library kvcore.sys of the component IOCTL Handler. The manipulation leads to denial of service. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224012.</p> <p><b>CVE ID : CVE-2023-1630</b></p>		
NULL Pointer Dereference	25-Mar-2023	5.5	<p>A vulnerability, which was classified as problematic, was found in JiangMin Antivirus 16.2.2022.418. This affects the function 0x222010 in the library kvcore.sys of the component IOCTL Handler. The manipulation leads to null pointer dereference. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The identifier VDB-224013 was assigned to this vulnerability.</p> <p><b>CVE ID : CVE-2023-1631</b></p>	N/A	A-JIA-JIAN-050423/812

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
<b>Vendor: joommasters</b>					
<b>Product: jms_blog</b>					
Affected Version(s): 2.5.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	PrestaShop jmsblog 2.5.5 was discovered to contain a SQL injection vulnerability. <b>CVE ID : CVE-2023-27034</b>	<a href="https://friends-of-presta.github.io/security-advisories/modules/2023/03/13/jmsblog.html">https://friends-of-presta.github.io/security-advisories/modules/2023/03/13/jmsblog.html</a>	A-JOO-JMS_-050423/813
Affected Version(s): 2.5.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	PrestaShop jmsblog 2.5.5 was discovered to contain a SQL injection vulnerability. <b>CVE ID : CVE-2023-27034</b>	<a href="https://friends-of-presta.github.io/security-advisories/modules/2023/03/13/jmsblog.html">https://friends-of-presta.github.io/security-advisories/modules/2023/03/13/jmsblog.html</a>	A-JOO-JMS_-050423/814
<b>Vendor: joomunited</b>					
<b>Product: wp_meta_seo</b>					
Affected Version(s): * Up to (excluding) 4.5.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Mar-2023	8.8	The WP Meta SEO WordPress plugin before 4.5.3 does not properly sanitize and escape inputs into SQL queries, leading to a blind SQL Injection vulnerability that can be exploited by subscriber+ users. <b>CVE ID : CVE-2023-0875</b>	N/A	A-JOO-WP_M-050423/815

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
URL Redirection to Untrusted Site ('Open Redirect')	20-Mar-2023	6.1	The WP Meta SEO WordPress plugin before 4.5.3 does not authorize several ajax actions, allowing low-privilege users to make updates to certain data and leading to an arbitrary redirect vulnerability.  <b>CVE ID : CVE-2023-0876</b>	N/A	A-JOO-WP_M-050423/816
<b>Vendor: json-smart_project</b>					
<b>Product: json-smart</b>					
Affected Version(s): 2.4.9					
Uncontrolled Recursion	22-Mar-2023	7.5	[json-smart](https://netplex.github.io/json-smart/) is a performance focused, JSON processor lib. When reaching a '[' or '{' character in the JSON input, the code parses an array or an object respectively. It was discovered that the code does not have any limit to the nesting of such arrays or objects. Since the parsing of nested arrays and objects is done recursively, nesting too many of them can cause a stack exhaustion (stack overflow) and crash the software.  <b>CVE ID : CVE-2023-1370</b>	N/A	A-JSO-JSON-050423/817

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
<b>Vendor: judging_management_system_project</b>					
<b>Product: judging_management_system</b>					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	A vulnerability was found in SourceCodester Judging Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file summary_results.php. The manipulation of the argument main_event_id 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-223549 was assigned to this vulnerability. <b>CVE ID : CVE-2023-1556</b>	N/A	A-JUD-JUDG-050423/818
<b>Vendor: kaml_project</b>					
<b>Product: kaml</b>					
Affected Version(s): * Up to (excluding) 0.53.0					
Improper Restriction of Recursive Entity References in DTDs ('XML Entity')	20-Mar-2023	7.5	kaml provides YAML support for kotlinx.serialization. Prior to version 0.53.0, applications that use kaml to parse untrusted input containing anchors and aliases may consume excessive	<a href="https://github.com/charleskorn/kaml/security/advisories/GHSA-c24f-2j3g-rg48">https://github.com/charleskorn/kaml/security/advisories/GHSA-c24f-2j3g-rg48</a> , <a href="https://github.com/">https://github.com/</a>	A-KAM-KAML-050423/819

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
Expansion' )			memory and crash. Version 0.53.0 and later default to refusing to parse YAML documents containing anchors and aliases. There are no known workarounds.  <b>CVE ID : CVE-2023-28118</b>	harleskorn /kaml/commit/5f82a2d7e00bfc307afca05d1dc4d7c50593531a	
<b>Vendor: klaviyo</b>					
<b>Product: klaviyo</b>					
Affected Version(s): * Up to (including) 3.0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Klaviyo, Inc. Klaviyo plugin <= 3.0.7 versions.  <b>CVE ID : CVE-2023-25456</b>	N/A	A-KLA-KLAV-050423/820
<b>Vendor: knplabs</b>					
<b>Product: snappy</b>					
Affected Version(s): * Up to (excluding) 1.4.2					
Deserialization of Untrusted Data	17-Mar-2023	9.8	Snappy is a PHP library allowing thumbnail, snapshot or PDF generation from a url or a html page. Prior to version 1.4.2, Snappy is vulnerable to PHAR deserialization due to a lack of checking on the protocol before passing it into the `file_exists()` function. If an attacker can upload files of any	<a href="https://github.com/KnpLabs/snappy/security/advisories/GHSA-gq6w-q6wh-jggc">https://github.com/KnpLabs/snappy/security/advisories/GHSA-gq6w-q6wh-jggc</a> , <a href="https://github.com/KnpLabs/snappy/commit/b66f79334421c26d9c24442796">https://github.com/KnpLabs/snappy/commit/b66f79334421c26d9c24442796</a>	A-KNP-SNAP-050423/821

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
			<p>type to the server he can pass in the phar:// protocol to unserialize the uploaded file and instantiate arbitrary PHP objects. This can lead to remote code execution especially when snappy is used with frameworks with documented POP chains like Laravel/Symfony vulnerable developer code. If a user can control the output file from the <code>`generateFromHtml()`</code> function, it will invoke deserialization. This vulnerability is capable of remote code execution if Snappy is used with frameworks or developer code with vulnerable POP chains. It has been fixed in version 1.4.2.</p> <p><b>CVE ID : CVE-2023-28115</b></p>	<p>3fa2d92980b5d3,  <a href="https://github.com/KnpLabs/snappy/commit/1ee6360cbd5a5d09705909a150df7963a88efd6">https://github.com/KnpLabs/snappy/commit/1ee6360cbd5a5d09705909a150df7963a88efd6</a></p>	
<b>Vendor: ladybirdweb</b>					
<b>Product: faveo_helpdesk</b>					
Affected Version(s): From (including) 1.0 Up to (including) 1.11.1					
Improper Neutralization of Special Elements used in an SQL	24-Mar-2023	8.8	<p>Faveo Helpdesk 1.0-1.11.1 is vulnerable to SQL Injection. When the user logs in through the login box, he has no judgment on the validity of the</p>	N/A	A-LAD-FAVE-050423/822

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			user's input data. The parameters passed from the front end to the back end are controllable, which will lead to SQL injection. <b>CVE ID : CVE-2023-25350</b>		
<b>Product: faveo_servicedesk</b>					
Affected Version(s): 5.0.1					
Authorization Bypass Through User-Controlled Key	24-Mar-2023	6.5	Faveo 5.0.1 allows remote attackers to obtain sensitive information via a modified user ID in an Insecure Direct Object Reference (IDOR) attack. <b>CVE ID : CVE-2023-24625</b>	N/A	A-LAD-FAVE-050423/823
<b>Vendor: leadgenerated</b>					
<b>Product: lead_generated</b>					
Affected Version(s): * Up to (excluding) 1.25					
Deserialization of Untrusted Data	22-Mar-2023	9.8	The Lead Generated WordPress Plugin, version <= 1.23, was affected by an unauthenticated insecure deserialization issue. The tve_labels parameter of the tve_api_form_submit action is passed to the PHP unserialize() function without being sanitized or verified, and as a result could lead to PHP object injection, which when	N/A	A-LEA-LEAD-050423/824

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
			combined with certain class implementations / gadget chains could be leveraged to perform a variety of malicious actions granted a POP chain is also present. <b>CVE ID : CVE-2023-28667</b>		
<b>Vendor: lfpjects</b>					
<b>Product: mlflow</b>					
Affected Version(s): * Up to (excluding) 2.2.1					
Path Traversal: '..filename'	24-Mar-2023	9.8	Path Traversal: '\\.\filename' in GitHub repository mlflow/mlflow prior to 2.2.1. <b>CVE ID : CVE-2023-1177</b>	https://huntr.dev/bounties/1fe8f21a-c438-4cba-9add-e8a5dab94e28, https://github.com/mlflow/mlflow/commit/7162a50c654792c21f3e4a160eb1a0e6a34f6e6e	A-LFP-MLFL-050423/825
Affected Version(s): * Up to (excluding) 2.2.2					
Absolute Path Traversal	24-Mar-2023	3.3	Absolute Path Traversal in GitHub repository mlflow/mlflow prior to 2.2.2. <b>CVE ID : CVE-2023-1176</b>	https://huntr.dev/bounties/ae92f814-6a08-435c-8445-eec0ef4f1085, https://github.com/mlflow/mlflow/commit/	A-LFP-MLFL-050423/826

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
				63ef72aa4 334a6473c e7f889573 c92fcae0b3 c0d	
<b>Vendor: liblouis</b>					
<b>Product: liblouis</b>					
Affected Version(s): 3.24.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Mar-2023	7.5	Buffer Overflow vulnerability found in Liblouis v.3.24.0 allows a remote attacker to cause a denial of service via the lou_logFile function at logginc.c endpoint. <b>CVE ID : CVE-2023-26767</b>	<a href="https://github.com/liblouis/liblouis/issues/1292">https://github.com/liblouis/liblouis/issues/1292</a> , <a href="https://github.com/liblouis/liblouis/pull/1297">https://github.com/liblouis/liblouis/pull/1297</a>	A-LIB-LIBL-050423/827
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Mar-2023	7.5	Buffer Overflow vulnerability found in Liblouis v.3.24.0 allows a remote attacker to cause a denial of service via the compileTranslationTable.c and lou_setDataPath functions. <b>CVE ID : CVE-2023-26768</b>	<a href="https://github.com/liblouis/liblouis/pull/1302">https://github.com/liblouis/liblouis/pull/1302</a>	A-LIB-LIBL-050423/828
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Mar-2023	7.5	Buffer Overflow vulnerability found in Liblouis Lou_Trace v.3.24.0 allows a remote attacker to cause a denial of service via the resolveSubtable function at	<a href="https://github.com/liblouis/liblouis/pull/1300">https://github.com/liblouis/liblouis/pull/1300</a>	A-LIB-LIBL-050423/829

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
			compileTranslationTabel.c. <b>CVE ID : CVE-2023-26769</b>		
<b>Vendor: lightcms_project</b>					
<b>Product: lightcms</b>					
Affected Version(s): 1.3.7					
N/A	22-Mar-2023	9.8	LightCMS v1.3.7 was discovered to contain a remote code execution (RCE) vulnerability via the image:make function. <b>CVE ID : CVE-2023-27060</b>	<a href="https://github.com/eddy8/LightCMS/issues/21">https://github.com/eddy8/LightCMS/issues/21</a>	A-LIG-LIGH-050423/830
<b>Vendor: loan_management_system_project</b>					
<b>Product: loan_management_system</b>					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Mar-2023	5.4	SourceCodester Loan Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the Type parameter under the Edit Loan Types module. <b>CVE ID : CVE-2023-27242</b>	N/A	A-LOA-LOAN-050423/831
<b>Vendor: mage-people</b>					
<b>Product: event_manager_and_tickets_selling_for_woocommerce</b>					
Affected Version(s): * Up to (excluding) 3.8.7					
Improper Neutralization of Input During Web Page Generation	23-Mar-2023	4.8	Auth. (admin+) Stored Cross-site Scripting (XSS) vulnerability in MagePeople Team Event Manager and Tickets Selling Plugin	N/A	A-MAG-EVEN-050423/832

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 Scripting')			for WooCommerce <= 3.8.6. versions. <b>CVE ID : CVE-2023-28422</b>		
<b>Vendor: mainwp</b>					
<b>Product: code_snippets_extension</b>					
Affected Version(s): * Up to (excluding) 4.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	5.4	Auth. (subscriber+) Stored Cross-Site Scripting (XSS) vulnerability in MainWP MainWP Code Snippets Extension plugin <= 4.0.2 versions. <b>CVE ID : CVE-2023-23650</b>	N/A	A-MAI-CODE-050423/833
<b>Vendor: Malwarebytes</b>					
<b>Product: adwcleaner</b>					
Affected Version(s): * Up to (including) 8.4.0					
Improper Link Resolution Before File Access ('Link Following')	29-Mar-2023	7.8	Malwarebytes AdwCleaner 8.4.0 runs as Administrator and performs an insecure file delete operation on C:\AdwCleaner\Logs\AdwCleaner_Debug.log in which the target location is user-controllable, allowing a non-admin user to escalate privileges to SYSTEM via a symbolic link. <b>CVE ID : CVE-2023-28892</b>	<a href="https://www.malwarebytes.com/secure/cves/cve-2023-28892">https://www.malwarebytes.com/secure/cves/cve-2023-28892</a>	A-MAL-ADWC-050423/834
<b>Product: malwarebytes</b>					
Affected Version(s): * Up to (excluding) 4.5.23					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Link Resolution Before File Access ('Link Following')	23-Mar-2023	7.8	In Malwarebytes before 4.5.23, a symbolic link may be used delete any arbitrary file on the system by exploiting the local quarantine system. It can also lead to privilege escalation in certain scenarios. <b>CVE ID : CVE-2023-26088</b>	<a href="https://www.malwarebytes.com/secure/cves/cve-2023-26088">https://www.malwarebytes.com/secure/cves/cve-2023-26088</a>	A-MAL-MALW-050423/835
<b>Vendor: mattermost</b>					
<b>Product: mattermost</b>					
Affected Version(s): * Up to (excluding) 7.5.0					
Exposure of Resource to Wrong Sphere	22-Mar-2023	4.3	Mattermost fails to check the "Show Full Name" setting when rendering the result for the /plugins/focalboard/api/v2/users API call, allowing an attacker to learn the full name of a board owner. <b>CVE ID : CVE-2023-1562</b>	<a href="https://mattermost.com/security-updates/">https://mattermost.com/security-updates/</a>	A-MAT-MATT-050423/836
<b>Vendor: maxpcsecure</b>					
<b>Product: anti_virus_plus</b>					
Affected Version(s): 19.0.2.1					
Improper Access Control	18-Mar-2023	5.5	A vulnerability was found in Max Secure Anti Virus Plus 19.0.2.1 and classified as critical. Affected by this issue is the function 0x220020 in the library SDActMon.sys of the component	N/A	A-MAX-ANTI-050423/837

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
			IoControlCode Handler. The manipulation leads to improper access controls. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223376. <b>CVE ID : CVE-2023-1490</b>		
Improper Access Control	18-Mar-2023	5.5	A vulnerability was found in Max Secure Anti Virus Plus 19.0.2.1. It has been classified as critical. This affects the function 0x220020 in the library MaxCryptMon.sys of the component IoControlCode Handler. The manipulation leads to improper access controls. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-223377 was assigned to this vulnerability. <b>CVE ID : CVE-2023-1491</b>	N/A	A-MAX-ANTI-050423/838
Improper Resource	18-Mar-2023	5.5	A vulnerability was found in Max Secure Anti Virus Plus 19.0.2.1. It has been	N/A	A-MAX-ANTI-050423/839

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
Shutdown or Release			<p>declared as problematic. This vulnerability affects the function 0x220019 in the library MaxProc64.sys of the component IoControlCode Handler. The manipulation of the argument SystemBuffer leads to denial of service. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. VDB-223378 is the identifier assigned to this vulnerability.</p> <p><b>CVE ID : CVE-2023-1492</b></p>		
Improper Resource Shutdown or Release	18-Mar-2023	5.5	<p>A vulnerability was found in Max Secure Anti Virus Plus 19.0.2.1. It has been rated as problematic. This issue affects the function 0x220019 in the library MaxProctetor64.sys of the component IoControlCode Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The associated</p>	N/A	A-MAX-ANTI-050423/840

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
			<p>identifier of this vulnerability is VDB-223379.</p> <p><b>CVE ID : CVE-2023-1493</b></p>		
<b>Vendor: McAfee</b>					
<b>Product: total_protection</b>					
Affected Version(s): * Up to (excluding) 16.0.50					
N/A	21-Mar-2023	6.7	<p>McAfee Total Protection prior to 16.0.50 may allow an adversary (with full administrative access) to modify a McAfee specific Component Object Model (COM) in the Windows Registry. This can result in the loading of a malicious payload.</p> <p><b>CVE ID : CVE-2023-25134</b></p>	<p><a href="https://www.mcafee.com/support/?articleId=TS103398&amp;page=shell&amp;shell=article-view">https://www.mcafee.com/support/?articleId=TS103398&amp;page=shell&amp;shell=article-view</a>,  <a href="https://www.mcafee.com/en-us/consumer-corporate/mcafee-labs/product-security-bulletins.html">https://www.mcafee.com/en-us/consumer-corporate/mcafee-labs/product-security-bulletins.html</a></p>	A-MCA-TOTA-050423/841
<b>Vendor: medical_certificate_generator_app_project</b>					
<b>Product: medical_certificate_generator_app</b>					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	<p>A vulnerability was found in SourceCodester Medical Certificate Generator App 1.0. It has been declared as critical. This vulnerability affects unknown code of the file action.php. The manipulation of the</p>	N/A	A-MED-MEDI-050423/842

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-223558 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1566</b>		
<b>Vendor: medicine_tracker_system_project</b>					
<b>Product: medicine_tracker_system</b>					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Medicine Tracker System 1.0. This issue affects some unknown processing of the file medicines/view_detail.s.php of the component GET Parameter Handler. The manipulation of the argument GET 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-223283. <b>CVE ID : CVE-2023-1439</b>	N/A	A-MED-MEDI-050423/843

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 Authentication	17-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Medicine Tracker System 1.0. This affects an unknown part of the file Users.php?f=save_user. The manipulation of the argument firstname/middlename/lastname/username/password leads to improper authentication. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-223311. <b>CVE ID : CVE-2023-1464</b>	N/A	A-MED-MEDI-050423/844
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Mar-2023	6.1	A vulnerability, which was classified as problematic, has been found in SourceCodester Medicine Tracker System 1.0. Affected by this issue is some unknown functionality of the file app/?page=medicines/manage_medicine. The manipulation of the argument name/description with the input <script>alert('2')</script> leads to cross site scripting. The attack may be launched	N/A	A-MED-MEDI-050423/845

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
			remotely. The identifier of this vulnerability is VDB-223292. <b>CVE ID : CVE-2023-1447</b>		
<b>Vendor: megamain</b>					
<b>Product: mega_main_menu</b>					
Affected Version(s): * Up to (including) 2.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Mar-2023	4.8	The Mega Main Menu plugin for WordPress is vulnerable to Stored Cross-Site Scripting via some of its settings parameters in versions up to, and including, 2.2.2 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. This only affects multi-site installations and installations where unfiltered_html has been disabled. <b>CVE ID : CVE-2023-1575</b>	N/A	A-MEG-MEGA-050423/846
<b>Vendor: menu_shortcode_project</b>					
<b>Product: menu_shortcode</b>					
Affected Version(s): * Up to (including) 1.0					

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')	27-Mar-2023	5.4	The menu shortcode WordPress plugin through 1.0 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0395</b>	N/A	A-MEN-MENU-050423/847

**Vendor: metagauss**

**Product: profilegrid**

Affected Version(s): \* Up to (excluding) 5.3.1

Incorrect Authorization	20-Mar-2023	8.8	The ProfileGrid WordPress plugin before 5.3.1 provides an AJAX endpoint for resetting a user password but does not implement proper authorization. This allows a user with low privileges, such as subscriber, to change the password of any account, including Administrator ones. <b>CVE ID : CVE-2023-0940</b>	N/A	A-MET-PROF-050423/848
-------------------------	-------------	-----	--	-----	-----------------------

**Vendor: mgt-commerce**

**Product: cloudpanel**

Affected Version(s): \* Up to (excluding) 2.2.1

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	21-Mar-2023	8.1	MGT-COMMERCE CloudPanel ships with a static SSL certificate to encrypt communications to the administrative interface, shared across every installation of CloudPanel. This behavior was observed in version 2.2.0. There has been no indication from the vendor this has been addressed in version 2.2.1.  <b>CVE ID : CVE-2023-0391</b>	N/A	A-MGT-CLOU-050423/849
<b>Vendor: miniflux_project</b>					
<b>Product: miniflux</b>					
Affected Version(s): * Up to (excluding) 2.0.43					
N/A	17-Mar-2023	7.5	Miniflux is a feed reader. Prior to version 2.0.43, an unauthenticated user can retrieve Prometheus metrics from a publicly reachable Miniflux instance where the `METRICS_COLLECTOR` configuration option is enabled and `METRICS_ALLOWED_NETWORKS` is set to `127.0.0.1/8` (the default). A patch is available in Miniflux 2.0.43. As a workaround, set `METRICS_COLLECTOR`	<a href="https://github.com/miniflux/v2/security/advisories/GHSA-3qjf-qh38-x73v">https://github.com/miniflux/v2/security/advisories/GHSA-3qjf-qh38-x73v</a> , <a href="https://github.com/miniflux/v2/pull/1745">https://github.com/miniflux/v2/pull/1745</a>	A-MIN-MINI-050423/850

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
			R` to `false` (default) or run Miniflux behind a trusted reverse-proxy. <b>CVE ID : CVE-2023-27591</b>		
Affected Version(s): From (including) 2.0.25 Up to (excluding) 2.0.43					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Mar-2023	5.4	Miniflux is a feed reader. Since v2.0.25, Miniflux will automatically proxy images served over HTTP to prevent mixed content errors. When an outbound request made by the Go HTTP client fails, the `html.ServerError` is returned unescaped without the expected Content Security Policy header added to valid responses. By creating an RSS feed item with the inline description containing an `` tag with a `srcset` attribute pointing to an invalid URL like `http:a<script>alert(1)</script>`, we can coerce the proxy handler into an error condition where the invalid URL is returned unescaped and in full. This results in JavaScript execution on the Miniflux instance as soon as the user is convinced (e.g. by a	<a href="https://github.com/miniflux/v2/pull/1746">https://github.com/miniflux/v2/pull/1746</a> , <a href="https://github.com/miniflux/v2/security/advisories/GHSA-mqqg-xjhj-wfgw">https://github.com/miniflux/v2/security/advisories/GHSA-mqqg-xjhj-wfgw</a>	A-MIN-MINI-050423/851

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
			<p>message in the alt text) to open the broken image. An attacker can execute arbitrary JavaScript in the context of a victim Miniflux user when they open a broken image in a crafted RSS feed. This can be used to perform actions on the Miniflux instance as that user and gain administrative access to the Miniflux instance if it is reachable and the victim is an administrator. A patch is available in version 2.0.43. As a workaround disable image proxy; default value is `http-only`.</p> <p><b>CVE ID : CVE-2023-27592</b></p>		

**Vendor: minio**

**Product: minio**

Affected Version(s): \* Up to (excluding) 2023-03-20t20-16-18z

N/A	22-Mar-2023	8.8	<p>Minio is a Multi-Cloud Object Storage framework. All users on Windows prior to version RELEASE.2023-03-20T20-16-18Z are impacted. MinIO fails to filter the `` character, which allows for arbitrary object placement across buckets. As a</p>	<p><a href="https://github.com/minio/minio/commit/8d6558b23649f613414c8527b58973fbdfa4d1b8">https://github.com/minio/minio/commit/8d6558b23649f613414c8527b58973fbdfa4d1b8</a>,  <a href="https://github.com/minio/minio/security/a">https://github.com/minio/minio/security/a</a></p>	A-MIN-MINI-050423/852
-----	-------------	-----	---	--	-----------------------

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
			<p>result, a user with low privileges, such as an access key, service account, or STS credential, which only has permission to `PutObject` in a specific bucket, can create an admin user. This issue is patched in RELEASE.2023-03-20T20-16-18Z. There are no known workarounds.</p> <p><b>CVE ID : CVE-2023-28433</b></p>	<p>dvisories/GHSA-w23q-4hw3-2pp6,  <a href="https://github.com/minio/minio/commit/b3c54ec81e0a06392abfb3a1ffcdc80c6fbf6ebc">https://github.com/minio/minio/commit/b3c54ec81e0a06392abfb3a1ffcdc80c6fbf6ebc</a></p>	
N/A	22-Mar-2023	8.8	<p>Minio is a Multi-Cloud Object Storage framework. Prior to RELEASE.2023-03-20T20-16-18Z, an attacker can use crafted requests to bypass metadata bucket name checking and put an object into any bucket while processing `PostPolicyBucket`. To carry out this attack, the attacker requires credentials with `arn:aws:s3:::*` permission, as well as enabled Console API access. This issue has been patched in RELEASE.2023-03-20T20-16-18Z. As a workaround, enable browser API access and turn off</p>	<p><a href="https://github.com/minio/minio/security/advisories/GHSA-2pxw-r47w-4p8c">https://github.com/minio/minio/security/advisories/GHSA-2pxw-r47w-4p8c</a>,  <a href="https://github.com/minio/minio/commit/67f4ba154a27a1b06e48bfabda38355a010dfca5">https://github.com/minio/minio/commit/67f4ba154a27a1b06e48bfabda38355a010dfca5</a></p>	A-MIN-MINI-050423/853

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
			<pre>`MINIO_BROWSER=off`</pre> <p><b>CVE ID : CVE-2023-28434</b></p>		
Affected Version(s): From (including) 2019-12-17t23-16-33z Up to (excluding) 2023-03-20t20-16-18z					
N/A	22-Mar-2023	7.5	<p>Minio is a Multi-Cloud Object Storage framework. In a cluster deployment starting with RELEASE.2019-12-17T23-16-33Z and prior to RELEASE.2023-03-20T20-16-18Z, MinIO returns all environment variables, including `MINIO_SECRET_KEY` and `MINIO_ROOT_PASSWORD`, resulting in information disclosure. All users of distributed deployment are impacted. All users are advised to upgrade to RELEASE.2023-03-20T20-16-18Z.</p> <p><b>CVE ID : CVE-2023-28432</b></p>	<p><a href="https://github.com/minio/minio/security/advisories/GHSA-6xvq-wj2x-3h3q">https://github.com/minio/minio/security/advisories/GHSA-6xvq-wj2x-3h3q</a></p>	A-MIN-MINI-050423/854
<b>Vendor: miniorange</b>					
<b>Product: oauth_single_sign_on</b>					
Affected Version(s): * Up to (excluding) 6.24.2					
Cross-Site Request Forgery (CSRF)	27-Mar-2023	6.5	<p>The OAuth Single Sign On WordPress plugin before 6.24.2 does not have CSRF checks when discarding</p>	N/A	A-MIN-OAUT-050423/855

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Identify providers (IdP), which could allow attackers to make logged in admins delete all IdP via a CSRF attack <b>CVE ID : CVE-2023-1093</b>		
<b>Vendor: mirotalk</b>					
<b>Product: mirotalk_p2p</b>					
Affected Version(s): * Up to (excluding) 2023-02-18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	6.1	A cross-site scripting (XSS) vulnerability in MiroTalk P2P before commit f535b35 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter under the settings module. <b>CVE ID : CVE-2023-27054</b>	<a href="https://github.com/miroslavpejic85/mirotalk/issues/139">https://github.com/miroslavpejic85/mirotalk/issues/139</a> , <a href="https://github.com/miroslavpejic85/mirotalk/commit/f535b3515d2d480dc3135b37982f5df93e43c592">https://github.com/miroslavpejic85/mirotalk/commit/f535b3515d2d480dc3135b37982f5df93e43c592</a>	A-MIR-MIRO-050423/856
<b>Vendor: Misp-project</b>					
<b>Product: malware_information_sharing_platform</b>					
Affected Version(s): * Up to (excluding) 2.4.169					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Mar-2023	6.1	js/event-graph.js in MISP before 2.4.169 allows XSS via event-graph node tooltips. <b>CVE ID : CVE-2023-28606</b>	<a href="https://github.com/MISP/MISP/commit/30255b8d683df4ec54f856282b3bde9106d5ae1a">https://github.com/MISP/MISP/commit/30255b8d683df4ec54f856282b3bde9106d5ae1a</a>	A-MIS-MALW-050423/857

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')	18-Mar-2023	6.1	js/event-graph.js in MISP before 2.4.169 allows XSS via the event-graph relationship tooltip. <b>CVE ID : CVE-2023-28607</b>	<a href="https://github.com/MISP/MISP/commit/78f423451a4c795991e739ee970bc5215c061591">https://github.com/MISP/MISP/commit/78f423451a4c795991e739ee970bc5215c061591</a>	A-MIS-MALW-050423/858
Affected Version(s): 2.4.169					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	In MISP 2.4.169, app/Lib/Tools/CustomPaginationTool.php allows XSS in the community index. <b>CVE ID : CVE-2023-28884</b>	<a href="https://github.com/MISP/MISP/commit/b94c7978e5e6b1db369abeedbbf00bca975b08b7">https://github.com/MISP/MISP/commit/b94c7978e5e6b1db369abeedbbf00bca975b08b7</a>	A-MIS-MALW-050423/859
<b>Vendor: monitoring_of_students_cyber_accounts_system_project</b>					
<b>Product: monitoring_of_students_cyber_accounts_system</b>					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Mar-2023	9.8	A vulnerability classified as critical was found in SourceCodester Monitoring of Students Cyber Accounts System 1.0. Affected by this vulnerability is an unknown functionality of the file login.php of the component POST Parameter Handler. The manipulation of the argument un leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be	N/A	A-MON-MONI-050423/860

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. The associated identifier of this vulnerability is VDB-223363. <b>CVE ID : CVE-2023-1480</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Mar-2023	6.1	A vulnerability, which was classified as problematic, has been found in SourceCodester Monitoring of Students Cyber Accounts System 1.0. Affected by this issue is some unknown functionality of the file modules/balance/index.php?view=balancelist of the component POST Parameter Handler. The manipulation of the argument id with the input "><script>alert(111)</script> leads to cross site scripting. 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-223364. <b>CVE ID : CVE-2023-1481</b>	N/A	A-MON-MONI-050423/861
<b>Vendor: monospace</b>					
<b>Product: directus</b>					
Affected Version(s): * Up to (excluding) 9.23.3					

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
Improper Access Control	24-Mar-2023	5.5	<p>Directus is a real-time API and App dashboard for managing SQL database content. Prior to version 9.23.3, the `directus_refresh_token` is not redacted properly from the log outputs and can be used to impersonate users without their permission. This issue is patched in version 9.23.3.</p> <p><b>CVE ID : CVE-2023-28443</b></p>	<p><a href="https://github.com/directus/directus/security/advisories/GHSA-8vg2-wf3q-mwv7">https://github.com/directus/directus/security/advisories/GHSA-8vg2-wf3q-mwv7</a>,  <a href="https://github.com/directus/directus/commit/349536303983ccba68ecb3e4fb35315424011afc">https://github.com/directus/directus/commit/349536303983ccba68ecb3e4fb35315424011afc</a></p>	A-MON-DIRE-050423/862
<b>Vendor: Moodle</b>					
<b>Product: moodle</b>					
Affected Version(s): 4.1.1					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	<p>The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS).</p> <p><b>CVE ID : CVE-2023-28333</b></p>	<p><a href="https://moodle.org/mod/forum/discuss.php?id=445065">https://moodle.org/mod/forum/discuss.php?id=445065</a></p>	A-MOO-MOOD-050423/863
Improper Neutralization of Special Elements used in an SQL Command	23-Mar-2023	8.8	<p>Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers).</p>	<p><a href="https://moodle.org/mod/forum/discuss.php?id=445061">https://moodle.org/mod/forum/discuss.php?id=445061</a></p>	A-MOO-MOOD-050423/864

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			<b>CVE ID : CVE-2023-28329</b>		
Cross-Site Request Forgery (CSRF)	23-Mar-2023	8.8	The link to reset all templates of a database activity did not include the necessary token to prevent a CSRF risk. <b>CVE ID : CVE-2023-28335</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445067">https://moodle.org/mod/forum/discuss.php?d=445067</a>	A-MOO-MOOD-050423/865
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to teachers, managers and admins by default. <b>CVE ID : CVE-2023-28330</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445062">https://moodle.org/mod/forum/discuss.php?d=445062</a>	A-MOO-MOOD-050423/866
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. <b>CVE ID : CVE-2023-28331</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445063">https://moodle.org/mod/forum/discuss.php?d=445063</a>	A-MOO-MOOD-050423/867
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk. <b>CVE ID : CVE-2023-28332</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445064">https://moodle.org/mod/forum/discuss.php?d=445064</a>	A-MOO-MOOD-050423/868
Exposure of Resource	23-Mar-2023	4.3	The course participation report required additional	<a href="https://moodle.org/mod/forum/">https://moodle.org/mod/forum/</a>	A-MOO-MOOD-050423/869

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			checks to prevent roles being displayed which the user did not have access to view. <b>CVE ID : CVE-2023-1402</b>	discuss.php?d=445069	
Authorization Bypass Through User-Controlled Key	23-Mar-2023	4.3	Authenticated users were able to enumerate other users' names via the learning plans page. <b>CVE ID : CVE-2023-28334</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445066">https://moodle.org/mod/forum/discuss.php?d=445066</a>	A-M00-MOOD-050423/870
Affected Version(s): 3.11.0					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS). <b>CVE ID : CVE-2023-28333</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445065">https://moodle.org/mod/forum/discuss.php?d=445065</a>	A-M00-MOOD-050423/871
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers). <b>CVE ID : CVE-2023-28329</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445061">https://moodle.org/mod/forum/discuss.php?d=445061</a>	A-M00-MOOD-050423/872
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is	<a href="https://moodle.org/mod/forum/discuss.php?d=445062">https://moodle.org/mod/forum/discuss.php?d=445062</a>	A-M00-MOOD-050423/873

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
			only available to teachers, managers and admins by default. <b>CVE ID : CVE-2023-28330</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. <b>CVE ID : CVE-2023-28331</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445063">https://moodle.org/mod/forum/discuss.php?d=445063</a>	A-MOO-MOOD-050423/874
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk. <b>CVE ID : CVE-2023-28332</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445064">https://moodle.org/mod/forum/discuss.php?d=445064</a>	A-MOO-MOOD-050423/875
Exposure of Resource to Wrong Sphere	23-Mar-2023	4.3	The course participation report required additional checks to prevent roles being displayed which the user did not have access to view. <b>CVE ID : CVE-2023-1402</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445069">https://moodle.org/mod/forum/discuss.php?d=445069</a>	A-MOO-MOOD-050423/876
Affected Version(s): 3.9.0					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploita	<a href="https://moodle.org/mod/forum/discuss.php?d=445065">https://moodle.org/mod/forum/discuss.php?d=445065</a>	A-MOO-MOOD-050423/877

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
			ble anywhere in the core Moodle LMS). <b>CVE ID : CVE-2023-28333</b>		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers). <b>CVE ID : CVE-2023-28329</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445061">https://moodle.org/mod/forum/discuss.php?d=445061</a>	A-MOO-MOOD-050423/878
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to teachers, managers and admins by default. <b>CVE ID : CVE-2023-28330</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445062">https://moodle.org/mod/forum/discuss.php?d=445062</a>	A-MOO-MOOD-050423/879
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. <b>CVE ID : CVE-2023-28331</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445063">https://moodle.org/mod/forum/discuss.php?d=445063</a>	A-MOO-MOOD-050423/880
Improper Neutralization of Input During Web Page Generation	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk.	<a href="https://moodle.org/mod/forum/discuss.php?d=445064">https://moodle.org/mod/forum/discuss.php?d=445064</a>	A-MOO-MOOD-050423/881

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 Scripting')			<b>CVE ID : CVE-2023-28332</b>		
Exposure of Resource to Wrong Sphere	23-Mar-2023	4.3	The course participation report required additional checks to prevent roles being displayed which the user did not have access to view. <b>CVE ID : CVE-2023-1402</b>	<a href="https://moodle.org/mod/forum/discuss.php?id=445069">https://moodle.org/mod/forum/discuss.php?id=445069</a>	A-MOO-MOOD-050423/882
Affected Version(s): 4.0.0					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS). <b>CVE ID : CVE-2023-28333</b>	<a href="https://moodle.org/mod/forum/discuss.php?id=445065">https://moodle.org/mod/forum/discuss.php?id=445065</a>	A-MOO-MOOD-050423/883
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers). <b>CVE ID : CVE-2023-28329</b>	<a href="https://moodle.org/mod/forum/discuss.php?id=445061">https://moodle.org/mod/forum/discuss.php?id=445061</a>	A-MOO-MOOD-050423/884
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to	<a href="https://moodle.org/mod/forum/discuss.php?id=445062">https://moodle.org/mod/forum/discuss.php?id=445062</a>	A-MOO-MOOD-050423/885

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
			teachers, managers and admins by default. <b>CVE ID : CVE-2023-28330</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. <b>CVE ID : CVE-2023-28331</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445063">https://moodle.org/mod/forum/discuss.php?d=445063</a>	A-MOO-MOOD-050423/886
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk. <b>CVE ID : CVE-2023-28332</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445064">https://moodle.org/mod/forum/discuss.php?d=445064</a>	A-MOO-MOOD-050423/887
Exposure of Resource to Wrong Sphere	23-Mar-2023	4.3	The course participation report required additional checks to prevent roles being displayed which the user did not have access to view. <b>CVE ID : CVE-2023-1402</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445069">https://moodle.org/mod/forum/discuss.php?d=445069</a>	A-MOO-MOOD-050423/888
Authorization Bypass Through User-Controlled Key	23-Mar-2023	4.3	Authenticated users were able to enumerate other users' names via the learning plans page. <b>CVE ID : CVE-2023-28334</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445066">https://moodle.org/mod/forum/discuss.php?d=445066</a>	A-MOO-MOOD-050423/889
Affected Version(s): 4.1.0					

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 Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS). <b>CVE ID : CVE-2023-28333</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445065">https://moodle.org/mod/forum/discuss.php?d=445065</a>	A-MOO-MOOD-050423/890
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers). <b>CVE ID : CVE-2023-28329</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445061">https://moodle.org/mod/forum/discuss.php?d=445061</a>	A-MOO-MOOD-050423/891
Cross-Site Request Forgery (CSRF)	23-Mar-2023	8.8	The link to reset all templates of a database activity did not include the necessary token to prevent a CSRF risk. <b>CVE ID : CVE-2023-28335</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445067">https://moodle.org/mod/forum/discuss.php?d=445067</a>	A-MOO-MOOD-050423/892
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to teachers, managers and admins by default. <b>CVE ID : CVE-2023-28330</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445062">https://moodle.org/mod/forum/discuss.php?d=445062</a>	A-MOO-MOOD-050423/893

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')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. <b>CVE ID : CVE-2023-28331</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445063">https://moodle.org/mod/forum/discuss.php?d=445063</a>	A-MOO-MOOD-050423/894
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk. <b>CVE ID : CVE-2023-28332</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445064">https://moodle.org/mod/forum/discuss.php?d=445064</a>	A-MOO-MOOD-050423/895
Exposure of Resource to Wrong Sphere	23-Mar-2023	4.3	The course participation report required additional checks to prevent roles being displayed which the user did not have access to view. <b>CVE ID : CVE-2023-1402</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445069">https://moodle.org/mod/forum/discuss.php?d=445069</a>	A-MOO-MOOD-050423/896
Authorization Bypass Through User-Controlled Key	23-Mar-2023	4.3	Authenticated users were able to enumerate other users' names via the learning plans page. <b>CVE ID : CVE-2023-28334</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445066">https://moodle.org/mod/forum/discuss.php?d=445066</a>	A-MOO-MOOD-050423/897
Affected Version(s): From (excluding) 3.11.0 Up to (excluding) 3.11.13					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did	<a href="https://moodle.org/mod/forum/discuss.php?d=445065">https://moodle.org/mod/forum/discuss.php?d=445065</a>	A-MOO-MOOD-050423/898

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
			not appear to be implemented/exploitable anywhere in the core Moodle LMS). <b>CVE ID : CVE-2023-28333</b>		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers). <b>CVE ID : CVE-2023-28329</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445061">https://moodle.org/mod/forum/discuss.php?d=445061</a>	A-MOO-MOOD-050423/899
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to teachers, managers and admins by default. <b>CVE ID : CVE-2023-28330</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445062">https://moodle.org/mod/forum/discuss.php?d=445062</a>	A-MOO-MOOD-050423/900
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. <b>CVE ID : CVE-2023-28331</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445063">https://moodle.org/mod/forum/discuss.php?d=445063</a>	A-MOO-MOOD-050423/901
Improper Neutralization of Input During Web Page Generation	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the	<a href="https://moodle.org/mod/forum/discuss.php?d=445064">https://moodle.org/mod/forum/discuss.php?d=445064</a>	A-MOO-MOOD-050423/902

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 Scripting')			server), it presented an XSS risk. <b>CVE ID : CVE-2023-28332</b>		
Exposure of Resource to Wrong Sphere	23-Mar-2023	4.3	The course participation report required additional checks to prevent roles being displayed which the user did not have access to view. <b>CVE ID : CVE-2023-1402</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445069">https://moodle.org/mod/forum/discuss.php?d=445069</a>	A-MOO-MOOD-050423/903
Affected Version(s): From (excluding) 3.9.0 Up to (excluding) 3.9.20					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS). <b>CVE ID : CVE-2023-28333</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445065">https://moodle.org/mod/forum/discuss.php?d=445065</a>	A-MOO-MOOD-050423/904
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers). <b>CVE ID : CVE-2023-28329</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445061">https://moodle.org/mod/forum/discuss.php?d=445061</a>	A-MOO-MOOD-050423/905
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is	<a href="https://moodle.org/mod/forum/discuss.php?d=445062">https://moodle.org/mod/forum/discuss.php?d=445062</a>	A-MOO-MOOD-050423/906

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
			only available to teachers, managers and admins by default. <b>CVE ID : CVE-2023-28330</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. <b>CVE ID : CVE-2023-28331</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445063">https://moodle.org/mod/forum/discuss.php?d=445063</a>	A-MOO-MOOD-050423/907
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk. <b>CVE ID : CVE-2023-28332</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445064">https://moodle.org/mod/forum/discuss.php?d=445064</a>	A-MOO-MOOD-050423/908
Exposure of Resource to Wrong Sphere	23-Mar-2023	4.3	The course participation report required additional checks to prevent roles being displayed which the user did not have access to view. <b>CVE ID : CVE-2023-1402</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445069">https://moodle.org/mod/forum/discuss.php?d=445069</a>	A-MOO-MOOD-050423/909
Affected Version(s): From (excluding) 4.0.0 Up to (excluding) 4.0.7					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploita	<a href="https://moodle.org/mod/forum/discuss.php?d=445065">https://moodle.org/mod/forum/discuss.php?d=445065</a>	A-MOO-MOOD-050423/910

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
			ble anywhere in the core Moodle LMS). <b>CVE ID : CVE-2023-28333</b>		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers). <b>CVE ID : CVE-2023-28329</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445061">https://moodle.org/mod/forum/discuss.php?d=445061</a>	A-MOO-MOOD-050423/911
N/A	23-Mar-2023	6.5	Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to teachers, managers and admins by default. <b>CVE ID : CVE-2023-28330</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445062">https://moodle.org/mod/forum/discuss.php?d=445062</a>	A-MOO-MOOD-050423/912
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk. <b>CVE ID : CVE-2023-28331</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445063">https://moodle.org/mod/forum/discuss.php?d=445063</a>	A-MOO-MOOD-050423/913
Improper Neutralization of Input During Web Page Generation	23-Mar-2023	6.1	If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk.	<a href="https://moodle.org/mod/forum/discuss.php?d=445064">https://moodle.org/mod/forum/discuss.php?d=445064</a>	A-MOO-MOOD-050423/914

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 Scripting')			<b>CVE ID : CVE-2023-28332</b>		
Exposure of Resource to Wrong Sphere	23-Mar-2023	4.3	The course participation report required additional checks to prevent roles being displayed which the user did not have access to view. <b>CVE ID : CVE-2023-1402</b>	<a href="https://moodle.org/mod/forum/discuss.php?id=445069">https://moodle.org/mod/forum/discuss.php?id=445069</a>	A-MOO-MOOD-050423/915
Authorization Bypass Through User-Controlled Key	23-Mar-2023	4.3	Authenticated users were able to enumerate other users' names via the learning plans page. <b>CVE ID : CVE-2023-28334</b>	<a href="https://moodle.org/mod/forum/discuss.php?id=445066">https://moodle.org/mod/forum/discuss.php?id=445066</a>	A-MOO-MOOD-050423/916
<b>Vendor: mp4v2_project</b>					
<b>Product: mp4v2</b>					
Affected Version(s): 2.1.2					
Improper Resource Shutdown or Release	17-Mar-2023	5.5	A vulnerability was found in MP4v2 2.1.2 and classified as problematic. This issue affects the function DumpTrack of the file mp4trackdump.cpp. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223295.	N/A	A-MP4-MP4V-050423/917

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
			<b>CVE ID : CVE-2023-1450</b>		
Improper Resource Shutdown or Release	17-Mar-2023	5.5	A vulnerability was found in MP4v2 2.1.2. It has been classified as problematic. Affected is the function mp4v2::impl::MP4Track::GetSampleFileOffset of the file mp4track.cpp. The manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223296. <b>CVE ID : CVE-2023-1451</b>	N/A	A-MP4-MP4V-050423/918
<b>Vendor: Netgate</b>					
<b>Product: Pfsense</b>					
Affected Version(s): 2.7.0					
XML Injection (aka Blind XPath Injection)	17-Mar-2023	8.8	A command injection vulnerability in the function restore_rrddata() of Netgate pfSense v2.7.0 allows authenticated attackers to execute arbitrary commands via manipulating the contents of an XML file supplied to the component config.xml. <b>CVE ID : CVE-2023-27253</b>	<a href="https://redmine.pfsense.org/issues/13935">https://redmine.pfsense.org/issues/13935</a> , <a href="https://github.com/pfsense/pfsense/commit/ca80d18493f8f91b21933ebd6b714215ae1e5e94">https://github.com/pfsense/pfsense/commit/ca80d18493f8f91b21933ebd6b714215ae1e5e94</a>	A-NET-PFSE-050423/919

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
<b>Product: pfsense_plus</b>					
Affected Version(s): 22.05.1					
Improper Restriction of Excessive Authentication Attempts	22-Mar-2023	9.8	Improper restriction of excessive authentication attempts in the SSHGuard component of Netgate pfSense Plus software v22.05.1 and pfSense CE software v2.6.0 allows attackers to bypass brute force protection mechanisms via crafted web requests. <b>CVE ID : CVE-2023-27100</b>	<a href="https://redmine.pfsense.org/issues/13574">https://redmine.pfsense.org/issues/13574</a> , <a href="https://docs.netgate.com/downloads/pfSense-SA-23_05.sshguard.asc">https://docs.netgate.com/downloads/pfSense-SA-23_05.sshguard.asc</a>	A-NET-PFSE-050423/920
<b>Vendor: Nextcloud</b>					
<b>Product: nextcloud_server</b>					
Affected Version(s): From (including) 21.0.0 Up to (excluding) 21.0.9					
Improper Restriction of Excessive Authentication Attempts	22-Mar-2023	7.8	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Enterprise Server is the enterprise version of the file server software. In Nextcloud Server versions 25.0.x prior to 25.0.5 and versions 24.0.x prior to 24.0.10 as well as Nextcloud Enterprise Server versions 25.0.x prior to 25.0.4, 24.0.x prior to 24.0.10, 23.0.x prior to 23.0.12.5, 22.x prior to 22.2.0.10, and 21.x prior to 21.0.9.10,	<a href="https://github.com/nextcloud/security-advisories/security-advisories/GHSA-36g6-wjx2-333x">https://github.com/nextcloud/security-advisories/security-advisories/GHSA-36g6-wjx2-333x</a> , <a href="https://github.com/nextcloud/server/pull/36489">https://github.com/nextcloud/server/pull/36489</a>	A-NEX-NEXT-050423/921

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
			<p>when an attacker gets access to an already logged in user session they can then brute force the password on the confirmation endpoint. Nextcloud Server should be upgraded to 24.0.10 or 25.0.4 and Nextcloud Enterprise Server should be upgraded to 21.0.9.10, 22.2.10.10, 23.0.12.5, 24.0.10, or 25.0.4 to receive a patch. No known workarounds are available.</p> <p><b>CVE ID : CVE-2023-25820</b></p>		
Affected Version(s): From (including) 22.2.0 Up to (excluding) 22.2.10.10					
Improper Restriction of Excessive Authentication Attempts	22-Mar-2023	7.8	<p>Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Enterprise Server is the enterprise version of the file server software. In Nextcloud Server versions 25.0.x prior to 25.0.5 and versions 24.0.x prior to 24.0.10 as well as Nextcloud Enterprise Server versions 25.0.x prior to 25.0.4, 24.0.x prior to 24.0.10, 23.0.x prior to 23.0.12.5, 22.x prior to 22.2.0.10, and 21.x prior to 21.0.9.10,</p>	<p><a href="https://github.com/nextcloud/security-advisories/GHSA-36g6-wjx2-333x">https://github.com/nextcloud/security-advisories/GHSA-36g6-wjx2-333x</a>,  <a href="https://github.com/nextcloud/server/pull/36489">https://github.com/nextcloud/server/pull/36489</a></p>	A-NEX-NEXT-050423/922

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
			<p>when an attacker gets access to an already logged in user session they can then brute force the password on the confirmation endpoint. Nextcloud Server should be upgraded to 24.0.10 or 25.0.4 and Nextcloud Enterprise Server should be upgraded to 21.0.9.10, 22.2.10.10, 23.0.12.5, 24.0.10, or 25.0.4 to receive a patch. No known workarounds are available.</p> <p><b>CVE ID : CVE-2023-25820</b></p>		
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.12.5					
Improper Restriction of Excessive Authentication Attempts	22-Mar-2023	7.8	<p>Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Enterprise Server is the enterprise version of the file server software. In Nextcloud Server versions 25.0.x prior to 25.0.5 and versions 24.0.x prior to 24.0.10 as well as Nextcloud Enterprise Server versions 25.0.x prior to 25.0.4, 24.0.x prior to 24.0.10, 23.0.x prior to 23.0.12.5, 22.x prior to 22.2.0.10, and 21.x prior to 21.0.9.10,</p>	<p><a href="https://github.com/nextcloud/security-advisories/GHSA-36g6-wjx2-333x">https://github.com/nextcloud/security-advisories/GHSA-36g6-wjx2-333x</a>,  <a href="https://github.com/nextcloud/server/pull/36489">https://github.com/nextcloud/server/pull/36489</a></p>	A-NEX-NEXT-050423/923

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
			<p>when an attacker gets access to an already logged in user session they can then brute force the password on the confirmation endpoint. Nextcloud Server should be upgraded to 24.0.10 or 25.0.4 and Nextcloud Enterprise Server should be upgraded to 21.0.9.10, 22.2.10.10, 23.0.12.5, 24.0.10, or 25.0.4 to receive a patch. No known workarounds are available.</p> <p><b>CVE ID : CVE-2023-25820</b></p>		
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.10					
Improper Restriction of Excessive Authentication Attempts	22-Mar-2023	7.8	<p>Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Enterprise Server is the enterprise version of the file server software. In Nextcloud Server versions 25.0.x prior to 25.0.5 and versions 24.0.x prior to 24.0.10 as well as Nextcloud Enterprise Server versions 25.0.x prior to 25.0.4, 24.0.x prior to 24.0.10, 23.0.x prior to 23.0.12.5, 22.x prior to 22.2.0.10, and 21.x prior to 21.0.9.10,</p>	<p><a href="https://github.com/nextcloud/security-advisories/GHSA-36g6-wjx2-333x">https://github.com/nextcloud/security-advisories/GHSA-36g6-wjx2-333x</a>,  <a href="https://github.com/nextcloud/server/pull/36489">https://github.com/nextcloud/server/pull/36489</a></p>	A-NEX-NEXT-050423/924

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>when an attacker gets access to an already logged in user session they can then brute force the password on the confirmation endpoint. Nextcloud Server should be upgraded to 24.0.10 or 25.0.4 and Nextcloud Enterprise Server should be upgraded to 21.0.9.10, 22.2.10.10, 23.0.12.5, 24.0.10, or 25.0.4 to receive a patch. No known workarounds are available.</p> <p><b>CVE ID : CVE-2023-25820</b></p>		
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.9					
Incorrect Permission Assignment for Critical Resource	27-Mar-2023	8.1	<p>Nextcloud server is an open source, personal cloud implementation. In versions from 24.0.0 and before 24.0.9 a user could escalate their permissions to delete files they were not supposed to delete but only viewed or downloaded. This issue has been addressed and it is recommended that the Nextcloud Server is upgraded to 24.0.9. There are no known workarounds for this vulnerability.</p>	<p><a href="https://github.com/nextcloud/security-advisories/GHSA-8v5c-f752-fgpv">https://github.com/nextcloud/security-advisories/GHSA-8v5c-f752-fgpv</a>,  <a href="https://github.com/nextcloud/server/pull/33941">https://github.com/nextcloud/server/pull/33941</a></p>	A-NEX-NEXT-050423/925

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
			<b>CVE ID : CVE-2023-25817</b>		
Affected Version(s): From (including) 25.0.0 Up to (excluding) 25.0.4					
Improper Restriction of Excessive Authentication Attempts	22-Mar-2023	7.8	Nextcloud Server is the file server software for Nextcloud, a self-hosted productivity platform, and Nextcloud Enterprise Server is the enterprise version of the file server software. In Nextcloud Server versions 25.0.x prior to 25.0.5 and versions 24.0.x prior to 24.0.10 as well as Nextcloud Enterprise Server versions 25.0.x prior to 25.0.4, 24.0.x prior to 24.0.10, 23.0.x prior to 23.0.12.5, 22.x prior to 22.2.0.10, and 21.x prior to 21.0.9.10, when an attacker gets access to an already logged in user session they can then brute force the password on the confirmation endpoint. Nextcloud Server should be upgraded to 24.0.10 or 25.0.4 and Nextcloud Enterprise Server should be upgraded to 21.0.9.10, 22.2.10.10, 23.0.12.5, 24.0.10, or 25.0.4 to receive a patch. No known workarounds are available.	<a href="https://github.com/nextcloud/security-advisories/security-advisories/GHSA-36g6-wjx2-333x">https://github.com/nextcloud/security-advisories/GHSA-36g6-wjx2-333x</a> , <a href="https://github.com/nextcloud/server/pull/36489">https://github.com/nextcloud/server/pull/36489</a>	A-NEX-NEXT-050423/926

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
			<b>CVE ID : CVE-2023-25820</b>		
<b>Vendor: Nextendweb</b>					
<b>Product: smart_slider_3</b>					
Affected Version(s): * Up to (excluding) 3.5.1.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	The Smart Slider 3 WordPress plugin before 3.5.1.14 does not properly validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks  <b>CVE ID : CVE-2023-0660</b>	N/A	A-NEX-SMAR-050423/927
<b>Vendor: nooz_project</b>					
<b>Product: nooz</b>					
Affected Version(s): * Up to (including) 1.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	4.8	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Mighty Digital Nooz plugin <= 1.6.0 versions.  <b>CVE ID : CVE-2023-25794</b>	N/A	A-NOO-NOOZ-050423/928
<b>Vendor: notrinos</b>					
<b>Product: notrinoserp</b>					
Affected Version(s): 0.7					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	RESERVED NotrinosERP v0.7 was discovered to contain a SQL injection vulnerability via the OrderNumber parameter at /NotrinosERP/sales/customer_delivery.php. <b>CVE ID : CVE-2023-24788</b>	N/A	A-NOT-NOTR-050423/929
<b>Vendor: novel-plus_project</b>					
<b>Product: novel-plus</b>					
Affected Version(s): 3.6.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in novel-plus 3.6.2. Affected is the function MenuService of the file sys/menu/list. The manipulation of the argument sort leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-223662 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1594</b>	N/A	A-NOV-NOVE-050423/930
Improper Neutralization of Special Elements used in an SQL	23-Mar-2023	9.8	A vulnerability was found in novel-plus 3.6.2 and classified as critical. Affected by this issue is some unknown functionality of the file	N/A	A-NOV-NOVE-050423/931

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			DictController.java. The manipulation of the argument order by leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223736. <b>CVE ID : CVE-2023-1606</b>		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	8.8	A vulnerability was found in novel-plus 3.6.2. It has been classified as critical. This affects an unknown part of the file /common/sysFile/list. The manipulation of the argument sort 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-223737 was assigned to this vulnerability. <b>CVE ID : CVE-2023-1607</b>	N/A	A-NOV-NOVE-050423/932
Improper Neutralization of Special Elements used in an SQL Command	23-Mar-2023	7.2	A vulnerability has been found in novel-plus 3.6.2 and classified as critical. Affected by this vulnerability is an unknown functionality of the file	N/A	A-NOV-NOVE-050423/933

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			common/log/list. The manipulation of the argument sort leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223663. <b>CVE ID : CVE-2023-1595</b>		
<b>Vendor: nsthememes</b>					
<b>Product: advanced_social_pixel</b>					
Affected Version(s): * Up to (including) 2.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in NsThemes Advanced Social Pixel plugin <= 2.1.1 versions. <b>CVE ID : CVE-2023-24381</b>	N/A	A-NST-ADVA-050423/934
<b>Vendor: ofcms_project</b>					
<b>Product: ofcms</b>					
Affected Version(s): 1.1.4					
Improper Privilege Management	16-Mar-2023	8.8	An issue found in Ofcms v.1.1.4 allows a remote attacker to to escalate privileges via the respwd method in SysUserController. <b>CVE ID : CVE-2023-24760</b>	<a href="https://github.com/oufuf/ofcms/issues/16L75S">https://github.com/oufuf/ofcms/issues/16L75S</a>	A-OFC-OFCM-050423/935
<b>Vendor: omicronenergy</b>					
<b>Product: stationguard</b>					

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): * Up to (including) 2.20					
N/A	23-Mar-2023	9.8	The update process in OMICRON StationGuard and OMICRON StationScout before 2.21 can be exploited by providing a modified firmware update image. This allows a remote attacker to gain root access to the system. <b>CVE ID : CVE-2023-28610</b>	<a href="https://www.omicronenergy.com/fileadmin/user_upload/website/files/product-security/osa-5.txt">https://www.omicronenergy.com/fileadmin/user_upload/website/files/product-security/osa-5.txt</a> , <a href="https://www.omicronenergy.com/en/support/product-security/">https://www.omicronenergy.com/en/support/product-security/</a>	A-OMI-STAT-050423/936
Affected Version(s): From (including) 1.10 Up to (including) 2.20					
Incorrect Authorization	23-Mar-2023	9.8	Incorrect authorization in OMICRON StationGuard 1.10 through 2.20 and StationScout 1.30 through 2.20 allows an attacker to bypass intended access restrictions. <b>CVE ID : CVE-2023-28611</b>	<a href="https://www.omicronenergy.com/fileadmin/user_upload/website/files/product-security/osa-6.txt">https://www.omicronenergy.com/fileadmin/user_upload/website/files/product-security/osa-6.txt</a> , <a href="https://www.omicronenergy.com/en/support/product-security/">https://www.omicronenergy.com/en/support/product-security/</a>	A-OMI-STAT-050423/937
<b>Product: stationscout</b>					
Affected Version(s): * Up to (including) 2.20					
N/A	23-Mar-2023	9.8	The update process in OMICRON StationGuard and OMICRON StationScout before 2.21 can be exploited	<a href="https://www.omicronenergy.com/fileadmin/user_upload/website/">https://www.omicronenergy.com/fileadmin/user_upload/website/</a>	A-OMI-STAT-050423/938

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
			by providing a modified firmware update image. This allows a remote attacker to gain root access to the system. <b>CVE ID : CVE-2023-28610</b>	files/produ ct- security/os a-5.txt, https://ww w.omicrone nergy.com/ en/support /product- security/	
Affected Version(s): From (including) 1.30 Up to (including) 2.20					
Incorrect Authorization	23-Mar-2023	9.8	Incorrect authorization in OMICRON StationGuard 1.10 through 2.20 and StationScout 1.30 through 2.20 allows an attacker to bypass intended access restrictions. <b>CVE ID : CVE-2023-28611</b>	https://ww w.omicrone nergy.com/ fileadmin/ user_uploa d/website/ files/produ ct- security/os a-6.txt, https://ww w.omicrone nergy.com/ en/support /product- security/	A-OMI-STAT- 050423/939
<b>Vendor: onekeyadmin</b>					
<b>Product: onekeyadmin</b>					
Affected Version(s): 1.3.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-2023	5.4	onekeyadmin v1.3.9 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Member List module. <b>CVE ID : CVE-2023-26951</b>	N/A	A-ONE-ONEK- 050423/940
<b>Vendor: online_book_store_project_project</b>					
<b>Product: online_book_store_project</b>					

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): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Mar-2023	9.8	Online Book Store Project v1.0 is vulnerable to SQL Injection via /bookstore/bookPerPub.php. <b>CVE ID : CVE-2023-27250</b>	<a href="https://github.com/iknownt/bug_report/blob/main/vendors/itsourcecode.com/Online-Book-Store-Project/sql_injection.md">https://github.com/iknownt/bug_report/blob/main/vendors/itsourcecode.com/Online-Book-Store-Project/sql_injection.md</a>	A-ONL-ONLI-050423/941
<b>Vendor: online_exam_software_\ Product: _eexamhall_project</b>					
Affected Version(s): online_exam_software_\\ Up to (including) 4.0					
Cross-Site Request Forgery (CSRF)	20-Mar-2023	6.5	Cross-Site Request Forgery (CSRF) vulnerability in Aarvanshinfotech Online Exam Software: eExamhall plugin <= 4.0 versions. <b>CVE ID : CVE-2023-22681</b>	N/A	A-ONL-_EEX-050423/942
<b>Vendor: online_food_ordering_system_project Product: online_food_ordering_system</b>					
Affected Version(s): 2.0					
Improper Access Control	16-Mar-2023	9.8	A vulnerability was found in SourceCodester Online Food Ordering System 2.0 and classified as critical. Affected by this issue is some unknown functionality of the file /fos/admin/ajax.php?action=save_settings	N/A	A-ONL-ONLI-050423/943

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
			of the component POST Request Handler. The manipulation leads to improper access controls. The attack may be launched remotely. VDB-223214 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1432</b>		
<b>Vendor: online_pizza_ordering_system_project</b>					
<b>Product: online_pizza_ordering_system</b>					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability classified as critical was found in SourceCodester Online Pizza Ordering System 1.0. This vulnerability affects unknown code of the file admin/ajax.php?action=login2 of the component Login Page. The manipulation of the argument email with the input abc%40qq.com' AND (SELECT 9110 FROM (SELECT(SLEEP(5))))X Slc) AND 'jFNI'='jFNI leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The	N/A	A-ONL-ONLI-050423/944

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
			<p>identifier of this vulnerability is VDB-223300.</p> <p><b>CVE ID : CVE-2023-1455</b></p>		
Improper Authentication	17-Mar-2023	9.8	<p>A vulnerability was found in SourceCodester Online Pizza Ordering System 1.0. It has been classified as critical. This affects an unknown part of the file admin/ajax.php?action=save_user of the component Password Change Handler. The manipulation leads to improper authentication. It is possible to initiate the attack remotely. The identifier VDB-223305 was assigned to this vulnerability.</p> <p><b>CVE ID : CVE-2023-1460</b></p>	N/A	A-ONL-ONLI-050423/945

**Vendor: online\_tours\_\&\_travels\_management\_system\_project**

**Product: online\_tours\_\&\_travels\_management\_system**

Affected Version(s): 1.0

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	<p>A vulnerability has been found in SourceCodester Online Tours &amp; Travels Management System 1.0 and classified as critical. This vulnerability affects the function exec of the file admin/operations/ap</p>	N/A	A-ONL-ONLI-050423/946
--	-------------	-----	---	-----	-----------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>prove_delete.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-223654 is the identifier assigned to this vulnerability.</p> <p><b>CVE ID : CVE-2023-1589</b></p>		
<p>Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')</p>	23-Mar-2023	9.8	<p>A vulnerability was found in SourceCodester Online Tours &amp; Travels Management System 1.0 and classified as critical. This issue affects the function exec of the file admin/operations/currency.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-223655.</p> <p><b>CVE ID : CVE-2023-1590</b></p>	N/A	A-ONL-ONLI-050423/947
<b>Vendor: oohboi_steroids_for_elementor_project</b>					
<b>Product: oohboi_steroids_for_elementor</b>					
Affected Version(s): * Up to (excluding) 2.1.5					

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)	27-Mar-2023	6.5	The OoohBoi Steroids for Elementor WordPress plugin before 2.1.5 has CSRF and broken access control vulnerabilities which leads user with role as low as subscriber to delete attachment.  <b>CVE ID : CVE-2023-0336</b>	N/A	A-000-000H-050423/948
<b>Vendor: oospam</b>					
<b>Product: oospam_anti-spam</b>					
Affected Version(s): * Up to (excluding) 1.1.36					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	Auth. (admin+) Cross-Site Scripting vulnerability in OOPSpam OOPSpam Anti-Spam plugin <= 1.1.35 versions.  <b>CVE ID : CVE-2023-22716</b>	N/A	A-OOP-OOPS-050423/949
<b>Vendor: Openbsd</b>					
<b>Product: openssh</b>					
Affected Version(s): * Up to (excluding) 9.3					
N/A	17-Mar-2023	9.8	ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints.  <b>CVE ID : CVE-2023-28531</b>	N/A	A-OPE-OPEN-050423/950
<b>Vendor: openfind</b>					
<b>Product: mail2000</b>					
Affected Version(s): 8.0					

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')	27-Mar-2023	5.4	Openfind Mail2000 file uploading function has insufficient filtering for user input. An authenticated remote attacker with general user privilege can exploit this vulnerability to inject JavaScript, conducting an XSS attack.  <b>CVE ID : CVE-2023-22902</b>	<a href="https://www.twcert.org.tw/tw/cp-132-6953-79236-1.html">https://www.twcert.org.tw/tw/cp-132-6953-79236-1.html</a>	A-OPE-MAIL-050423/951
Affected Version(s): 7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	Openfind Mail2000 file uploading function has insufficient filtering for user input. An authenticated remote attacker with general user privilege can exploit this vulnerability to inject JavaScript, conducting an XSS attack.  <b>CVE ID : CVE-2023-22902</b>	<a href="https://www.twcert.org.tw/tw/cp-132-6953-79236-1.html">https://www.twcert.org.tw/tw/cp-132-6953-79236-1.html</a>	A-OPE-MAIL-050423/952
<b>Vendor: opengoofy</b>					
<b>Product: hippo4j</b>					
Affected Version(s): * Up to (excluding) 1.4.3					
Incorrect Permission Assignment for Critical Resource	16-Mar-2023	6.5	Insecure Permissions vulnerability found in OpenGoofy Hippo4j v.1.4.3 allows attacker to escalate privileges via the AddUser method of the UserController function in Tenant Management module.	N/A	A-OPE-HIPP-050423/953

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
			<b>CVE ID : CVE-2023-27095</b>		
Affected Version(s): 1.4.3					
N/A	23-Mar-2023	8.8	An issue found in OpenGoofy Hippo4j v.1.4.3 allows attackers to escalate privileges via the ThreadPoolController of the tenant Management module. <b>CVE ID : CVE-2023-27094</b>	<a href="https://github.com/penngoofy/hippo4j/issues/1059">https://github.com/penngoofy/hippo4j/issues/1059</a>	A-OPE-HIPP-050423/954
Incorrect Permission Assignment for Critical Resource	27-Mar-2023	6.5	Insecure Permissions vulnerability found in OpenGoofy Hippo4j v.1.4.3 allows attacker to obtain sensitive information via the ConfigVerifyController function of the Tenant Management module. <b>CVE ID : CVE-2023-27096</b>	<a href="https://github.com/penngoofy/hippo4j/issues/1060">https://github.com/penngoofy/hippo4j/issues/1060</a>	A-OPE-HIPP-050423/955
<b>Vendor: Opennms</b>					
<b>Product: horizon</b>					
Affected Version(s): * Up to (excluding) 31.0.6					
Cross-Site Request Forgery (CSRF)	22-Mar-2023	6.7	A form can be manipulated with cross-site request forgery in multiple versions of OpenNMS Meridian and Horizon. This can potentially allow an attacker to gain access to confidential information and compromise integrity. The solution is to upgrade to Meridian	<a href="https://github.com/OpenNMS/opennms/pull/5835/files">https://github.com/OpenNMS/opennms/pull/5835/files</a>	A-OPE-HORI-050423/956

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
			<p>2023.1.1 or Horizon 31.0.6 or newer.</p> <p>Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet.</p> <p><b>CVE ID : CVE-2023-0870</b></p>		
<b>Product: meridian</b>					
Affected Version(s): 2023.1.0					
Cross-Site Request Forgery (CSRF)	22-Mar-2023	6.7	<p>A form can be manipulated with cross-site request forgery in multiple versions of OpenNMS Meridian and Horizon. This can potentially allow an attacker to gain access to confidential information and compromise integrity. The solution is to upgrade to Meridian 2023.1.1 or Horizon 31.0.6 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet.</p>	<p><a href="https://github.com/OpenNMS/openNMS/pull/5835/files">https://github.com/OpenNMS/openNMS/pull/5835/files</a></p>	A-OPE-MERI-050423/957

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
			<b>CVE ID : CVE-2023-0870</b>		
Affected Version(s): From (including) 2020.1.0 Up to (excluding) 2020.1.33					
Cross-Site Request Forgery (CSRF)	22-Mar-2023	6.7	<p>A form can be manipulated with cross-site request forgery in multiple versions of OpenNMS Meridian and Horizon. This can potentially allow an attacker to gain access to confidential information and compromise integrity. The solution is to upgrade to Meridian 2023.1.1 or Horizon 31.0.6 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet.</p> <p><b>CVE ID : CVE-2023-0870</b></p>	<a href="https://github.com/OpenNMS/openNMS/pull/5835/files">https://github.com/OpenNMS/openNMS/pull/5835/files</a>	A-OPE-MERI-050423/958
Affected Version(s): From (including) 2021.1.0 Up to (excluding) 2021.1.25					
Cross-Site Request Forgery (CSRF)	22-Mar-2023	6.7	<p>A form can be manipulated with cross-site request forgery in multiple versions of OpenNMS Meridian and Horizon. This can potentially allow an attacker to gain access to confidential</p>	<a href="https://github.com/OpenNMS/openNMS/pull/5835/files">https://github.com/OpenNMS/openNMS/pull/5835/files</a>	A-OPE-MERI-050423/959

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
			<p>information and compromise integrity. The solution is to upgrade to Meridian 2023.1.1 or Horizon 31.0.6 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet.</p> <p><b>CVE ID : CVE-2023-0870</b></p>		
Affected Version(s): From (including) 2022.1.0 Up to (excluding) 2022.1.14					
Cross-Site Request Forgery (CSRF)	22-Mar-2023	6.7	<p>A form can be manipulated with cross-site request forgery in multiple versions of OpenNMS Meridian and Horizon. This can potentially allow an attacker to gain access to confidential information and compromise integrity. The solution is to upgrade to Meridian 2023.1.1 or Horizon 31.0.6 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly</p>	<p><a href="https://github.com/OpenNMS/opennms/pull/5835/files">https://github.com/OpenNMS/opennms/pull/5835/files</a></p>	A-OPE-MERI-050423/960

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
			accessible from the Internet. <b>CVE ID : CVE-2023-0870</b>		
<b>Vendor: Openssl</b>					
<b>Product: openssl</b>					
Affected Version(s): From (including) 1.0.2 Up to (excluding) 1.0.2zh					
Improper Certificate Validation	22-Mar-2023	7.5	A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the '-policy' argument to the command line utilities or by calling the 'X509_VERIFY_PARAM_set1_policies()' function. <b>CVE ID : CVE-2023-0464</b>	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2017771e2db3e2b96f89bbe8766c3209f6a99545">https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2017771e2db3e2b96f89bbe8766c3209f6a99545</a> , <a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=959c59c7a0164117e7f8366466a32bb1f8d77ff1">https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=959c59c7a0164117e7f8366466a32bb1f8d77ff1</a> , <a href="https://www.openssl.org/news/secadv/20230322.txt">https://www.openssl.org/news/secadv/20230322.txt</a>	A-OPE-OPEN-050423/961
Affected Version(s): From (including) 1.1.1 Up to (excluding) 1.1.1u					

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 Certificate Validation	22-Mar-2023	7.5	<p>A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the '-policy' argument to the command line utilities or by calling the 'X509_VERIFY_PARAM_set1_policies()' function.</p> <p><b>CVE ID : CVE-2023-0464</b></p>	<p><a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2017771e2db3e2b96f89bbe8766c3209f6a99545">https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2017771e2db3e2b96f89bbe8766c3209f6a99545</a>, <a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=959c59c7a0164117e7f8366466a32bb1f8d77ff1">https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=959c59c7a0164117e7f8366466a32bb1f8d77ff1</a>, <a href="https://www.openssl.org/news/secadv/20230322.txt">https://www.openssl.org/news/secadv/20230322.txt</a></p>	A-OPE-OPEN-050423/962
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.9					
Improper Certificate Validation	22-Mar-2023	7.5	<p>A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able</p>	<p><a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2017771e2db3e2b96f89bbe8766c3209f6a99545">https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2017771e2db3e2b96f89bbe8766c3209f6a99545</a>,</p>	A-OPE-OPEN-050423/963

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
			<p>to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the '-policy' argument to the command line utilities or by calling the 'X509_VERIFY_PARAM_set1_policies()' function.</p> <p><b>CVE ID : CVE-2023-0464</b></p>	<p><a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=959c59c7a0164117e7f8366466a32bb1f8d77ff1">https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=959c59c7a0164117e7f8366466a32bb1f8d77ff1</a>,  <a href="https://www.openssl.org/news/secadv/20230322.txt">https://www.openssl.org/news/secadv/20230322.txt</a></p>	
Affected Version(s): From (including) 3.1.0 Up to (excluding) 3.1.1					
Improper Certificate Validation	22-Mar-2023	7.5	<p>A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems.</p>	<p><a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2017771e2db3e2b96f89bbe8766c3209f6a99545">https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2017771e2db3e2b96f89bbe8766c3209f6a99545</a>,  <a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=959c59c7a0164117e7f8366466a32bb1f8d77ff1">https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=959c59c7a0164117e7f8366466a32bb1f8d77ff1</a>,</p>	A-OPE-OPEN-050423/964

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
			Policy processing is disabled by default but can be enabled by passing the '-policy' argument to the command line utilities or by calling the 'X509_VERIFY_PARAM_set1_policies()' function. <b>CVE ID : CVE-2023-0464</b>	<a href="https://www.openssl.org/news/secadv/20230322.txt">https://www.openssl.org/news/secadv/20230322.txt</a>	
<b>Vendor: otcms</b>					
<b>Product: otcms</b>					
Affected Version(s): 6.72					
Server-Side Request Forgery (SSRF)	25-Mar-2023	9.8	A vulnerability was found in OTCMS 6.72. It has been classified as critical. Affected is the function UseCurl of the file /admin/info_deal.php of the component URL Parameter Handler. The manipulation leads to server-side request forgery. 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-224016. <b>CVE ID : CVE-2023-1634</b>	N/A	A-OTC-OTCM-050423/965
Improper Neutralization of Input During	25-Mar-2023	6.1	A vulnerability was found in OTCMS 6.72. It has been declared as problematic. Affected by this vulnerability is	N/A	A-OTC-OTCM-050423/966

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			the function AutoRun of the file apiRun.php. The manipulation of the argument mode leads to cross site scripting. The attack can be launched remotely. The identifier VDB-224017 was assigned to this vulnerability. <b>CVE ID : CVE-2023-1635</b>		
<b>Vendor: Otrs</b>					
<b>Product: otrs</b>					
Affected Version(s): From (including) 6.0.1 Up to (including) 6.0.34					
Improper Control of Generation of Code ('Code Injection')	20-Mar-2023	7.8	Improper Input Validation vulnerability in OTRS AG OTRS (ACL modules), OTRS AG ((OTRS)) Community Edition (ACL modules) allows Local Execution of Code. When creating/importing an ACL it was possible to inject code that gets executed via manipulated comments and ACL-names This issue affects OTRS: from 7.0.X before 7.0.42, from 8.0.X before 8.0.31; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34. <b>CVE ID : CVE-2023-1250</b>	<a href="https://otrs.com/releases-notes/otrs-security-advisory-2023-02/">https://otrs.com/releases-notes/otrs-security-advisory-2023-02/</a>	A-OTR-OTRS-050423/967

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')	20-Mar-2023	6.1	Improper Input Validation vulnerability in OTRS AG OTRS (Ticket Actions modules), OTRS AG ((OTRS)) Community Edition (Ticket Actions modules) allows Cross-Site Scripting (XSS). This issue affects OTRS: from 7.0.X before 7.0.42; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34. <b>CVE ID : CVE-2023-1248</b>	<a href="https://otrs.com/release-notes/otrs-security-advisory-2023-01/">https://otrs.com/release-notes/otrs-security-advisory-2023-01/</a>	A-OTR-OTRS-050423/968
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.42					
Improper Control of Generation of Code ('Code Injection')	20-Mar-2023	7.8	Improper Input Validation vulnerability in OTRS AG OTRS (ACL modules), OTRS AG ((OTRS)) Community Edition (ACL modules) allows Local Execution of Code. When creating/importing an ACL it was possible to inject code that gets executed via manipulated comments and ACL-names This issue affects OTRS: from 7.0.X before 7.0.42, from 8.0.X before 8.0.31; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34.	<a href="https://otrs.com/release-notes/otrs-security-advisory-2023-02/">https://otrs.com/release-notes/otrs-security-advisory-2023-02/</a>	A-OTR-OTRS-050423/969

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
			<b>CVE ID : CVE-2023-1250</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	6.1	Improper Input Validation vulnerability in OTRS AG OTRS (Ticket Actions modules), OTRS AG ((OTRS)) Community Edition (Ticket Actions modules) allows Cross-Site Scripting (XSS). This issue affects OTRS: from 7.0.X before 7.0.42; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34. <b>CVE ID : CVE-2023-1248</b>	<a href="https://otrs.com/releases/notes/otrs-security-advisory-2023-01/">https://otrs.com/releases/notes/otrs-security-advisory-2023-01/</a>	A-OTR-OTRS-050423/970
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.0.31					
Improper Control of Generation of Code ('Code Injection')	20-Mar-2023	7.8	Improper Input Validation vulnerability in OTRS AG OTRS (ACL modules), OTRS AG ((OTRS)) Community Edition (ACL modules) allows Local Execution of Code. When creating/importing an ACL it was possible to inject code that gets executed via manipulated comments and ACL-names This issue affects OTRS: from 7.0.X before 7.0.42, from 8.0.X before 8.0.31; ((OTRS)) Community Edition:	<a href="https://otrs.com/releases/notes/otrs-security-advisory-2023-02/">https://otrs.com/releases/notes/otrs-security-advisory-2023-02/</a>	A-OTR-OTRS-050423/971

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
			from 6.0.1 through 6.0.34. <b>CVE ID : CVE-2023-1250</b>		
<b>Vendor: pacstrapor</b>					
<b>Product: pacstrapor</b>					
Affected Version(s): * Up to (excluding) 1.22					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Pacstrapor allows SQL Injection, Command Line Execution through SQL Injection. This issue affects Pacstrapor: before 1.22. <b>CVE ID : CVE-2023-1153</b>	N/A	A-PAC-PACS-050423/972
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Mar-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pacstrapor allows Reflected XSS. This issue affects Pacstrapor: before 1.22. <b>CVE ID : CVE-2023-1154</b>	N/A	A-PAC-PACS-050423/973
<b>Vendor: page_loading_effects_project</b>					
<b>Product: page_loading_effects</b>					
Affected Version(s): * Up to (including) 2.0.0					
Improper Neutralization	20-Mar-2023	4.8	Auth. (admin+) Cross-Site Scripting (XSS)	N/A	A-PAG-PAGE-050423/974

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
ion of Input During Web Page Generation ('Cross-site Scripting')			vulnerability in Esstat17 Page Loading Effects plugin <= 2.0.0 versions. <b>CVE ID : CVE-2023-23718</b>		
<b>Vendor: parity</b>					
<b>Product: frontier</b>					
Affected Version(s): * Up to (excluding) 2023-03-15					
Incorrect Calculation	22-Mar-2023	7.5	Frontier is an Ethereum compatibility layer for Substrate. Frontier's `modexp` precompile uses `num-bigint` crate under the hood. In the implementation prior to pull request 1017, the cases for modulus being even and modulus being odd are treated separately. Odd modulus uses the fast Montgomery multiplication, and even modulus uses the slow plain power algorithm. This gas cost discrepancy was not accounted for in the `modexp` precompile, leading to possible denial of service attacks. No fixes for `num-bigint` are currently available, and thus this issue is fixed in the short term by raising the gas costs for even modulus, and	<a href="https://github.com/paritytech/frontier/pull/1017">https://github.com/paritytech/frontier/pull/1017</a> , <a href="https://github.com/paritytech/frontier/commit/5af12e94d7dfc8a0208a290643a800f55de7b219">https://github.com/paritytech/frontier/commit/5af12e94d7dfc8a0208a290643a800f55de7b219</a> , <a href="https://github.com/paritytech/frontier/security/advisories/GHSA-fcmm-54jp-7vf6">https://github.com/paritytech/frontier/security/advisories/GHSA-fcmm-54jp-7vf6</a>	A-PAR-FRON-050423/975

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
			in the long term fixing it in `num-bigint` or switching to another modexp implementation. The short-term fix for Frontier is deployed at pull request 1017. There are no known workarounds aside from applying the fix. <b>CVE ID : CVE-2023-28431</b>		

**Vendor: park\_ticketing\_management\_system\_project**

**Product: park\_ticketing\_management\_system**

Affected Version(s): 1.0

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Mar-2023	9.8	Phpgurukul Park Ticketing Management System 1.0 is vulnerable to SQL Injection via the User Name parameter. <b>CVE ID : CVE-2023-26959</b>	N/A	A-PAR-PARK-050423/976
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	4.8	Phpgurukul Park Ticketing Management System 1.0 is vulnerable to Cross Site Scripting (XSS) via the Admin Name parameter. <b>CVE ID : CVE-2023-26958</b>	N/A	A-PAR-PARK-050423/977

**Vendor: pdfio\_project**

**Product: pdfio**

Affected Version(s): \* Up to (excluding) 1.1.1

Allocation of	20-Mar-2023	3.3	PDFio is a C library for reading and writing	<a href="https://github.com/m">https://github.com/m</a>	A-PDF-PDFI-050423/978
---------------	-------------	-----	--	---	-----------------------

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
Resources Without Limits or Throttling			PDF files. In versions 1.1.0 and prior, a denial of service vulnerability exists in the pdfio parser. Crafted pdf files can cause the program to run at 100% utilization and never terminate. This is different from CVE-2023-24808. A patch for this issue is available in version 1.1.1. <b>CVE ID : CVE-2023-28428</b>	ichaelrswet/pdfio/security/advisories/GHSA-68x8-9phf-j7jf, <a href="https://github.com/michaelrswet/pdfio/commit/97d4955666779dc5b0665e15dd951a5c12426a31">https://github.com/michaelrswet/pdfio/commit/97d4955666779dc5b0665e15dd951a5c12426a31</a>	

**Vendor: Pfsense**

**Product: pfsense**

Affected Version(s): 2.6.0

Improper Restriction of Excessive Authentication Attempts	22-Mar-2023	9.8	Improper restriction of excessive authentication attempts in the SSHGuard component of Netgate pfSense Plus software v22.05.1 and pfSense CE software v2.6.0 allows attackers to bypass brute force protection mechanisms via crafted web requests. <b>CVE ID : CVE-2023-27100</b>	<a href="https://redmine.pfsense.org/issues/13574">https://redmine.pfsense.org/issues/13574</a> , <a href="https://docs.netgate.com/downloads/pfSense-SA-23_05.sshguard.asc">https://docs.netgate.com/downloads/pfSense-SA-23_05.sshguard.asc</a>	A-PFS-PFSE-050423/979
---	-------------	-----	---	--	-----------------------

**Vendor: Pimcore**

**Product: pimcore**

Affected Version(s): \* Up to (excluding) 10.5.19

Improper Neutralization of	22-Mar-2023	8.8	SQL Injection in GitHub repository	<a href="https://huntr.dev/bounties/7e4">https://huntr.dev/bounties/7e4</a>	A-PIM-PIMC-050423/980
----------------------------	-------------	-----	------------------------------------	---	-----------------------

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
Special Elements used in an SQL Command ('SQL Injection')			pimcore/pimcore prior to 10.5.19. <b>CVE ID : CVE-2023-1578</b>	41a14-8e55-4ab4-932c-4dc56bb1bc2e, <a href="https://github.com/pimcore/pimcore/commit/367b74488808d71ec3f66f4ca9e8df5217c2c8d2">https://github.com/pimcore/pimcore/commit/367b74488808d71ec3f66f4ca9e8df5217c2c8d2</a>	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	8	Pimcore is an open source data and experience management platform. Prior to version 10.5.19, since a user with 'report' permission can already write arbitrary SQL queries and given the fact that this endpoint is using the GET method (no CSRF protection), an attacker can inject an arbitrary query by manipulating a user to click on a link. Users should upgrade to version 10.5.19 to receive a patch or, as a workaround, may apply the patch manually. <b>CVE ID : CVE-2023-28438</b>	<a href="https://github.com/pimcore/pimcore/security/advisories/GHSA-vf7q-g2pv-jxvx">https://github.com/pimcore/pimcore/security/advisories/GHSA-vf7q-g2pv-jxvx</a> , <a href="https://github.com/pimcore/pimcore/pull/14526">https://github.com/pimcore/pimcore/pull/14526</a> , <a href="https://github.com/pimcore/pimcore/commit/d1abadb181c88eba4bce1916f9077469d4ea2bc.patch">https://github.com/pimcore/pimcore/commit/d1abadb181c88eba4bce1916f9077469d4ea2bc.patch</a>	A-PIM-PIMC-050423/981
Improper Neutralization of	16-Mar-2023	7.8	Pimcore is an open source data and experience	<a href="https://github.com/pimcore/pim">https://github.com/pimcore/pim</a>	A-PIM-PIMC-050423/982

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
Special Elements used in an SQL Command ('SQL Injection')			management platform. Prior to version 10.5.19, quoting is not done properly in UUID DAO model. There is the theoretical possibility to inject custom SQL if the developer is using this methods with input data and not doing proper input validation in advance and so relies on the auto-quoting being done by the DAO class. Users should update to version 10.5.19 to receive a patch or, as a workaround, apply the patch manually.  <b>CVE ID : CVE-2023-28108</b>	core/security/advisories/GHSA-xc9p-r5qj-8xm9, <a href="https://github.com/pimcore/pimcore/commit/08e7ba56ae983c3c67ec563b6989b16ef8f35275.patch">https://github.com/pimcore/pimcore/commit/08e7ba56ae983c3c67ec563b6989b16ef8f35275.patch</a> , <a href="https://github.com/pimcore/pimcore/pull/14633">https://github.com/pimcore/pimcore/pull/14633</a>	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	6.1	Pimcore is an open source data and experience management platform. Versions prior to 10.5.19 have an unsecured tooltip field in DataObject class definition. This vulnerability has the potential to steal a user's cookie and gain unauthorized access to that user's account through the stolen cookie or redirect users to other malicious sites. Users should upgrade to version 10.5.19 or, as	<a href="https://github.com/pimcore/pimcore/pull/14574.patch">https://github.com/pimcore/pimcore/pull/14574.patch</a> , <a href="https://github.com/pimcore/pimcore/security/advisories/GHSA-rcg9-hrhx-6q69">https://github.com/pimcore/pimcore/security/advisories/GHSA-rcg9-hrhx-6q69</a> , <a href="https://github.com/pimcore/pimcore/pull/14574">https://github.com/pimcore/pimcore/pull/14574</a>	A-PIM-PIMC-050423/983

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
			a workaround, apply the patch manually. <b>CVE ID : CVE-2023-28429</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-2023	5.4	Cross-site Scripting (XSS) - Reflected in GitHub repository pimcore/pimcore prior to 10.5.19. <b>CVE ID : CVE-2023-1429</b>	<a href="https://huntr.dev/bounties/e0829fea-e458-47b8-84a3-a74476d9638f">https://huntr.dev/bounties/e0829fea-e458-47b8-84a3-a74476d9638f</a> , <a href="https://github.com/pimcore/pimcore/commit/7588c336edb24050656111b89d69e69cc9feb5f5">https://github.com/pimcore/pimcore/commit/7588c336edb24050656111b89d69e69cc9feb5f5</a>	A-PIM-PIMC-050423/984
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.19. <b>CVE ID : CVE-2023-1515</b>	<a href="https://huntr.dev/bounties/ae0f2ec4-a245-4d0b-9d4d-bd8310dd6282">https://huntr.dev/bounties/ae0f2ec4-a245-4d0b-9d4d-bd8310dd6282</a> , <a href="https://github.com/pimcore/pimcore/commit/44c6b37aa649a0e3105fa41f3d74a3e511acf964">https://github.com/pimcore/pimcore/commit/44c6b37aa649a0e3105fa41f3d74a3e511acf964</a>	A-PIM-PIMC-050423/985
Improper Neutralization of Input During	20-Mar-2023	4.8	Cross-site Scripting (XSS) - DOM in GitHub repository	<a href="https://huntr.dev/bounties/82a8ebd-4d15-">https://huntr.dev/bounties/82a8ebd-4d15-</a>	A-PIM-PIMC-050423/986

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			pimcore/pimcore prior to 10.5.19. <b>CVE ID : CVE-2023-1517</b>	9f91-6060c8fa5a0d, <a href="https://github.com/pimcore/pimcore/commit/3a22700dacd8a439cffcb208838a4199e732cff7">https://github.com/pimcore/pimcore/commit/3a22700dacd8a439cffcb208838a4199e732cff7</a>	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-2023	4.8	Pimcore is an open source data and experience management platform. Prior to version 10.5.19, an attacker can use cross-site scripting to send a malicious script to an unsuspecting user. Users may upgrade to version 10.5.19 to receive a patch or, as a workaround, apply the patch manually. <b>CVE ID : CVE-2023-28106</b>	<a href="https://github.com/pimcore/pimcore/commit/c59d0bf1d03a5037b586fe06230694fa3818dbf2">https://github.com/pimcore/pimcore/commit/c59d0bf1d03a5037b586fe06230694fa3818dbf2</a> , <a href="https://github.com/pimcore/pimcore/pull/14669.patch">https://github.com/pimcore/pimcore/pull/14669.patch</a> , <a href="https://github.com/pimcore/pimcore/security/advisories/GHSA-x5j3-mq9g-8jc8">https://github.com/pimcore/pimcore/security/advisories/GHSA-x5j3-mq9g-8jc8</a>	A-PIM-PIMC-050423/987
<b>Vendor: pixedelic</b>					
<b>Product: camera_slideshow</b>					
Affected Version(s): * Up to (including) 1.4.0.1					
Improper Neutralization of Input During	20-Mar-2023	6.1	Reflected Cross-Site Scripting (XSS) vulnerability in Manuel Masia   Pixedelic.Com Camera	N/A	A-PIX-CAME-050423/988

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			slideshow plugin <= 1.4.0.1 versions. <b>CVE ID : CVE-2023-22682</b>		
<b>Vendor: play-with-docker</b>					
<b>Product: play_with_docker</b>					
Affected Version(s): 0.0.1					
Authorization Bypass Through User-Controlled Key	16-Mar-2023	6.5	Play With Docker is a browser-based Docker playground. Versions 0.0.2 and prior are vulnerable to domain hijacking. Because CORS configuration was not correct, an attacker could use `play-with-docker.com` as an example and set the origin header in an http request as `evil-play-with-docker.com`. The domain would echo in response header, which successfully bypassed the CORS policy and retrieved basic user information. This issue has been fixed in commit ed82247c9ab7990ad76ec2bf1498c2b2830b6f1a. There are no known workarounds. <b>CVE ID : CVE-2023-28109</b>	<a href="https://github.com/play-with-docker/play-with-docker/commit/ed82247c9ab7990ad76ec2bf1498c2b2830b6f1a">https://github.com/play-with-docker/play-with-docker/commit/ed82247c9ab7990ad76ec2bf1498c2b2830b6f1a</a> , <a href="https://github.com/play-with-docker/security/advisories/GHSA-vq59-5x26-h639">https://github.com/play-with-docker/security/advisories/GHSA-vq59-5x26-h639</a>	A-PLA-PLAY-050423/989
Affected Version(s): 0.0.2					
Authorization Bypass	16-Mar-2023	6.5	Play With Docker is a browser-based Docker	<a href="https://github.com/play-with-docker/play-with-docker/commit/ed82247c9ab7990ad76ec2bf1498c2b2830b6f1a">https://github.com/play-with-docker/play-with-docker/commit/ed82247c9ab7990ad76ec2bf1498c2b2830b6f1a</a>	A-PLA-PLAY-050423/990

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Through User-Controlled Key			<p>playground. Versions 0.0.2 and prior are vulnerable to domain hijacking. Because CORS configuration was not correct, an attacker could use `play-with-docker.com` as an example and set the origin header in an http request as `evil-play-with-docker.com`. The domain would echo in response header, which successfully bypassed the CORS policy and retrieved basic user information. This issue has been fixed in commit ed82247c9ab7990ad76ec2bf1498c2b2830b6f1a. There are no known workarounds.</p> <p><b>CVE ID : CVE-2023-28109</b></p>	<p>ay-with-docker/play-with-docker/commit/ed82247c9ab7990ad76ec2bf1498c2b2830b6f1a, <a href="https://github.com/play-with-docker/play-with-docker/security/advisories/GHSA-vq59-5x26-h639">https://github.com/play-with-docker/play-with-docker/security/advisories/GHSA-vq59-5x26-h639</a></p>	

**Vendor: Pluck-cms**

**Product: pluck**

Affected Version(s): \* Up to (excluding) 4.7.16

Unrestricted Upload of File with Dangerous Type	27-Mar-2023	7.2	<p>Pluck CMS is vulnerable to an authenticated remote code execution (RCE) vulnerability through its "albums" module. Albums are used to create collections of images that can be inserted into web</p>	<p><a href="https://www.synopsys.com/blogs/software-security/pluck-cms-vulnerability/">https://www.synopsys.com/blogs/software-security/pluck-cms-vulnerability/</a></p>	A-PLU-PLUC-050423/991
---	-------------	-----	---	--	-----------------------

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
			<p>pages across the site. Albums allow the upload of various filetypes, which undergo a normalization process before being available on the site. Due to lack of file extension validation, it is possible to upload a crafted JPEG payload containing an embedded PHP web-shell. An attacker may navigate to it directly to achieve RCE on the underlying web server. Administrator credentials for the Pluck CMS web interface are required to access the albums module feature, and are thus required to exploit this vulnerability.</p> <p>CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C (8.2 High)</p> <p><b>CVE ID : CVE-2023-25828</b></p>		
Affected Version(s): 4.7.16					
Unrestricted Upload of File with Dangerous Type	27-Mar-2023	7.2	<p>Pluck CMS is vulnerable to an authenticated remote code execution (RCE) vulnerability through its "albums" module. Albums are used to create collections of images that can be</p>	<p><a href="https://www.synopsys.com/blogs/software-security/pluck-cms-vulnerability/">https://www.synopsys.com/blogs/software-security/pluck-cms-vulnerability/</a></p>	A-PLU-PLUC-050423/992

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
			<p>inserted into web pages across the site. Albums allow the upload of various filetypes, which undergo a normalization process before being available on the site. Due to lack of file extension validation, it is possible to upload a crafted JPEG payload containing an embedded PHP web-shell. An attacker may navigate to it directly to achieve RCE on the underlying web server. Administrator credentials for the Pluck CMS web interface are required to access the albums module feature, and are thus required to exploit this vulnerability.</p> <p>CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C (8.2 High)</p> <p><b>CVE ID : CVE-2023-25828</b></p>		

**Vendor: plugin**

**Product: waiting**

Affected Version(s): \* Up to (including) 0.6.2

Improper Neutralization of Special Elements	22-Mar-2023	8.8	The Waiting: One-click Countdowns WordPress Plugin, version <= 0.6.2, is affected by an	N/A	A-PLU-WAIT-050423/993
---	-------------	-----	---	-----	-----------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			authenticated SQL injection vulnerability in the pbc_down[meta][id] parameter of the pbc_save_downs action. <b>CVE ID : CVE-2023-28659</b>		
<b>Vendor: pluginus</b>					
<b>Product: inpost_gallery</b>					
Affected Version(s): * Up to (including) 2.1.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	The InPost Gallery WordPress plugin, in versions < 2.2.2, is affected by a reflected cross-site scripting vulnerability in the 'imgurl' parameter to the add_inpost_gallery_slide_item action, which can only be triggered by an authenticated user. <b>CVE ID : CVE-2023-28666</b>	N/A	A-PLU-INPO-050423/994
<b>Product: wordpress_meta_data_and_taxonomies_filter</b>					
Affected Version(s): * Up to (including) 1.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	The Meta Data and Taxonomies Filter WordPress plugin, in versions < 1.3.1, is affected by a reflected cross-site scripting vulnerability in the 'tax_name' parameter of the mdf_get_tax_options_in_widget action, which can only be triggered	N/A	A-PLU-WORD-050423/995

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
			by an authenticated user. <b>CVE ID : CVE-2023-28664</b>		
<b>Vendor: Postgresql</b>					
<b>Product: pgadmin_4</b>					
Affected Version(s): * Up to (excluding) 6.19					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Mar-2023	6.5	pgAdmin 4 versions prior to v6.19 contains a directory traversal vulnerability. A user of the product may change another user's settings or alter the database. <b>CVE ID : CVE-2023-0241</b>	<a href="https://github.com/pgadmin-org/pgadmin4/issues/5734">https://github.com/pgadmin-org/pgadmin4/issues/5734</a>	A-POS-PGAD-050423/996
<b>Vendor: Prestashop</b>					
<b>Product: eo_tags</b>					
Affected Version(s): From (including) 1.2.0 Up to (excluding) 1.3.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Mar-2023	9.8	The eo_tags package before 1.3.0 for PrestaShop allows SQL injection via an HTTP User-Agent or Referer header. <b>CVE ID : CVE-2023-27569</b>	N/A	A-PRE-EO_T-050423/997
Affected Version(s): From (including) 1.2.0 Up to (excluding) 1.4.19					
Improper Neutralization of Special Elements used in an SQL Command	21-Mar-2023	9.8	The eo_tags package before 1.4.19 for PrestaShop allows SQL injection via a crafted _ga cookie. <b>CVE ID : CVE-2023-27570</b>	<a href="https://security.profil-eo.com/cve/eo_tags_2023-27569-27570/">https://security.profil-eo.com/cve/eo_tags_2023-27569-27570/</a>	A-PRE-EO_T-050423/998

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')					
<b>Vendor: Qemu</b>					
<b>Product: qemu</b>					
Affected Version(s): * Up to (including) 7.2.0					
Allocation of Resources Without Limits or Throttling	23-Mar-2023	5.5	A flaw was found in the QEMU implementation of VMWare's paravirtual RDMA device. This flaw allows a crafted guest driver to allocate and initialize a huge number of page tables to be used as a ring of descriptors for CQ and async events, potentially leading to an out-of-bounds read and crash of QEMU. <b>CVE ID : CVE-2023-1544</b>	<a href="https://lists.nongnu.org/archive/html/qemu-devel/2023-03/msg00206.html">https://lists.nongnu.org/archive/html/qemu-devel/2023-03/msg00206.html</a> , <a href="https://bugzilla.redhat.com/show_bug.cgi?id=2180364">https://bugzilla.redhat.com/show_bug.cgi?id=2180364</a>	A-QEM-QEMU-050423/999
<b>Vendor: Qibosoft</b>					
<b>Product: qibocms</b>					
Affected Version(s): v7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Mar-2023	8.8	Qibosoft QiboCMS v7 was discovered to contain a remote code execution (RCE) vulnerability via the Get_Title function at label_set_rs.php <b>CVE ID : CVE-2023-27037</b>	<a href="https://github.com/dienamer/vuln/blob/main/2023-01-14.md">https://github.com/dienamer/vuln/blob/main/2023-01-14.md</a>	A-QIB-QIBO-050423/1000
<b>Vendor: qykcms</b>					
<b>Product: qykcms</b>					
Affected Version(s): 4.3.0					

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
Unrestricted Upload of File with Dangerous Type	17-Mar-2023	7.2	A vulnerability was found in Meizhou Qingyunke QYKCMS 4.3.0. It has been classified as problematic. This affects an unknown part of the file /admin_system/api.php of the component Update Handler. The manipulation of the argument downurl 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-223287. <b>CVE ID : CVE-2023-1442</b>	N/A	A-QYK-QYKC-050423/1001
<b>Vendor: Radare</b>					
<b>Product: radare2</b>					
Affected Version(s): * Up to (excluding) 5.8.6					
Uncontrolled Resource Consumption	23-Mar-2023	7.5	Denial of Service in GitHub repository radareorg/radare2 prior to 5.8.6. <b>CVE ID : CVE-2023-1605</b>	<a href="https://github.com/radareorg/radare2/commit/508a6307045441defd1bef0999a1f7052097613f">https://github.com/radareorg/radare2/commit/508a6307045441defd1bef0999a1f7052097613f</a> , <a href="https://huntr.dev/bounties/9dddcf5b-7dd4-46cc-">https://huntr.dev/bounties/9dddcf5b-7dd4-46cc-</a>	A-RAD-RADA-050423/1002

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
				abf9-172dce20bab2	
<b>Vendor: Rapid7</b>					
<b>Product: insightappsec</b>					
Affected Version(s): * Up to (excluding) 23.2.1					
Improper Control of Generation of Code ('Code Injection')	21-Mar-2023	8.8	An authenticated attacker can leverage an exposed getattr() method via a Jinja template to smuggle OS commands and perform other actions that are normally expected to be private methods. This issue was resolved in the Managed and SaaS deployments on February 1, 2023, and in version 23.2.1 of the Self-Managed version of InsightCloudSec. <b>CVE ID : CVE-2023-1304</b>	N/A	A-RAP-INSI-050423/1003
Improper Control of Generation of Code ('Code Injection')	21-Mar-2023	8.8	An authenticated attacker can leverage an exposed resource.db() accessor method to smuggle Python method calls via a Jinja template, which can lead to code execution. This issue was resolved in the Managed and SaaS deployments on February 1, 2023, and in version 23.2.1 of the Self-Managed	N/A	A-RAP-INSI-050423/1004

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
			version of InsightCloudSec. <b>CVE ID : CVE-2023-1306</b>		
N/A	21-Mar-2023	8.1	An authenticated attacker can leverage an exposed "box" object to read and write arbitrary files from disk, provided those files can be parsed as yaml or JSON. This issue was resolved in the Managed and SaaS deployments on February 1, 2023, and in version 23.2.1 of the Self-Managed version of InsightCloudSec. <b>CVE ID : CVE-2023-1305</b>	N/A	A-RAP-INSI-050423/1005
<b>Product: insightcloudsec</b>					
Affected Version(s): * Up to (excluding) 2023.02.01					
Improper Control of Generation of Code ('Code Injection')	21-Mar-2023	8.8	An authenticated attacker can leverage an exposed getattr() method via a Jinja template to smuggle OS commands and perform other actions that are normally expected to be private methods. This issue was resolved in the Managed and SaaS deployments on February 1, 2023, and in version 23.2.1 of the Self-Managed	N/A	A-RAP-INSI-050423/1006

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
			version of InsightCloudSec. <b>CVE ID : CVE-2023-1304</b>		
Improper Control of Generation of Code ('Code Injection')	21-Mar-2023	8.8	An authenticated attacker can leverage an exposed resource.db() accessor method to smuggle Python method calls via a Jinja template, which can lead to code execution. This issue was resolved in the Managed and SaaS deployments on February 1, 2023, and in version 23.2.1 of the Self-Managed version of InsightCloudSec. <b>CVE ID : CVE-2023-1306</b>	N/A	A-RAP-INSI-050423/1007
N/A	21-Mar-2023	8.1	An authenticated attacker can leverage an exposed "box" object to read and write arbitrary files from disk, provided those files can be parsed as yaml or JSON. This issue was resolved in the Managed and SaaS deployments on February 1, 2023, and in version 23.2.1 of the Self-Managed version of InsightCloudSec. <b>CVE ID : CVE-2023-1305</b>	N/A	A-RAP-INSI-050423/1008

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
<b>Product: insightvm</b>					
Affected Version(s): * Up to (excluding) 6.6.179					
URL Redirection to Untrusted Site ('Open Redirect')	20-Mar-2023	6.1	Rapid7 InsightVM versions 6.6.178 and lower suffers from an open redirect vulnerability, whereby an attacker has the ability to redirect the user to a site of the attacker's choice using the 'page' parameter of the 'data/console/redirect' component of the application. This issue was resolved in the February, 2023 release of version 6.6.179.  <b>CVE ID : CVE-2023-0681</b>	N/A	A-RAP-INSI-050423/1009
<b>Vendor: rapidload</b>					
<b>Product: rapidload_power-up_for_autooptimize</b>					
Affected Version(s): * Up to (excluding) 1.7.2					
Cross-Site Request Forgery (CSRF)	17-Mar-2023	6.3	The RapidLoad Power-Up for Autooptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on its AJAX actions. This makes it possible for unauthenticated attackers to invoke those functions, via forged request	N/A	A-RAP-RAPI-050423/1010

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			granted they can trick a site administrator into performing an action such as clicking on a link. Actions include resetting the API key, accessing or deleting log files, and deleting cache among others.  <b>CVE ID : CVE-2023-1472</b>		
<b>Vendor: react_webcam_project</b>					
<b>Product: react_webcam</b>					
Affected Version(s): * Up to (including) 1.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The React Webcam WordPress plugin through 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 could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.  <b>CVE ID : CVE-2023-0365</b>	N/A	A-REA-REAC-050423/1011
<b>Vendor: real.kit_project</b>					
<b>Product: real.kit</b>					
Affected Version(s): * Up to (excluding) 5.1.1					
Improper Neutralization of Input During Web Page	20-Mar-2023	5.4	The real.Kit WordPress plugin before 5.1.1 does not validate and escape some of its shortcode attributes before	N/A	A-REA-REAL-050423/1012

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0364</b>		
<b>Vendor: really-simple-plugins</b>					
<b>Product: complianz</b>					
Affected Version(s): * Up to (excluding) 6.4.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	The Complianz WordPress plugin before 6.4.2, Complianz Premium WordPress plugin before 6.4.2 do not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks <b>CVE ID : CVE-2023-1069</b>	N/A	A-REA-COMP-050423/1013
<b>Vendor: redis</b>					
<b>Product: redis</b>					
Affected Version(s): From (including) 7.0.8 Up to (excluding) 7.0.10					
Reachable Assertion	20-Mar-2023	5.5	Redis is an in-memory database that persists on disk. Starting in version 7.0.8 and prior	<a href="https://github.com/redis/redis/security/adv">https://github.com/redis/redis/security/adv</a>	A-RED-REDI-050423/1014

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to version 7.0.10, authenticated users can use the MSETNX command to trigger a runtime assertion and termination of the Redis server process. The problem is fixed in Redis version 7.0.10. <b>CVE ID : CVE-2023-28425</b>	isories/GH SA-mvmm-4vq6-vw8c, <a href="https://github.com/redis/redis/commit/48e0d4788434833b47892fe9f3d91be7687f25c9">https://github.com/redis/redis/commit/48e0d4788434833b47892fe9f3d91be7687f25c9</a>	

**Vendor: request\_project**

**Product: request**

Affected Version(s): \* Up to (including) 2.88.1

Server-Side Request Forgery (SSRF)	16-Mar-2023	6.1	<b>** UNSUPPORTED WHEN ASSIGNED **</b> The Request package through 2.88.1 for Node.js allows a bypass of SSRF mitigations via an attacker-controller server that does a cross-protocol redirect (HTTP to HTTPS, or HTTPS to HTTP). NOTE: This vulnerability only affects products that are no longer supported by the maintainer. <b>CVE ID : CVE-2023-28155</b>	<a href="https://doyenssec.com/resources/Doyensec_Advisory_RequestSSRF_Q12023.pdf">https://doyenssec.com/resources/Doyensec_Advisory_RequestSSRF_Q12023.pdf</a> , <a href="https://github.com/request/request/issues/3442">https://github.com/request/request/issues/3442</a> , <a href="https://github.com/request/request/pull/3444">https://github.com/request/request/pull/3444</a>	A-REQ-REQU-050423/1015
------------------------------------	-------------	-----	--	---	------------------------

**Vendor: responsive\_hotel\_site\_project**

**Product: responsive\_hotel\_site**

Affected Version(s): 1.0

Improper Neutralization of	19-Mar-2023	9.8	A vulnerability classified as critical has been found in	N/A	A-RES-RESP-050423/1016
----------------------------	-------------	-----	--	-----	------------------------

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
Special Elements used in an SQL Command ('SQL Injection')			code-projects Responsive Hotel Site 1.0. Affected is an unknown function of the file messages.php of the component Newsletter Log Handler. The manipulation of the argument title leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-223398 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1498</b>		
<b>Vendor: rifartek</b>					
<b>Product: iot_wall</b>					
Affected Version(s): 22					
Incorrect Authorization	27-Mar-2023	8.1	RIFARTEK IOT Wall has a vulnerability of incorrect authorization. An authenticated remote attacker with general user privilege is allowed to perform specific privileged function to access and modify all sensitive data. <b>CVE ID : CVE-2023-25017</b>	<a href="https://www.twcert.org.tw/tw/cp-132-6962-34ac1-1.html">https://www.twcert.org.tw/tw/cp-132-6962-34ac1-1.html</a>	A-RIF-IOT_-050423/1017
Improper Neutralization of Input	27-Mar-2023	5.4	RIFARTEK IOT Wall transportation function has insufficient filtering	<a href="https://www.twcert.org.tw/tw/cp-132-6963-">https://www.twcert.org.tw/tw/cp-132-6963-</a>	A-RIF-IOT_-050423/1018

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			for user input. An authenticated remote attacker with general user privilege can inject JavaScript to perform reflected XSS (Reflected Cross-site scripting) attack. <b>CVE ID : CVE-2023-25018</b>	7d2ee-1.html	
<b>Vendor: rockoa</b>					
<b>Product: rockoa</b>					
Affected Version(s): 2.3.2					
Unrestricted Upload of File with Dangerous Type	19-Mar-2023	8.8	A vulnerability, which was classified as critical, was found in RockOA 2.3.2. This affects the function runAction of the file acloudCosAction.php.S QL. The manipulation of the argument fileid 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 identifier VDB-223401 was assigned to this vulnerability. <b>CVE ID : CVE-2023-1501</b>	N/A	A-ROC-ROCK-050423/1019
<b>Vendor: Rockwellautomation</b>					
<b>Product: modbus_tcp_server_add_on_instructions</b>					
Affected Version(s): From (including) 2.00.00 Up to (excluding) 2.04.00					
Exposure of Sensitive Information to an	17-Mar-2023	4.3	Rockwell Automation Modbus TCP Server AOI prior to 2.04.00 is vulnerable to an	<a href="https://rockwellautomation.com/ap">https://rockwellautomation.com/ap</a>	A-ROC-MODB-050423/1020

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			<p>unauthorized user sending a malformed message that could cause the controller to respond with a copy of the most recent response to the last valid request. If exploited, an unauthorized user could read the connected device's Modbus TCP Server AOI information.</p> <p><b>CVE ID : CVE-2023-0027</b></p>	p/answers/answer_view/a_id/1138766	
<b>Product: thinmanager</b>					
Affected Version(s): 13.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	9.8	<p>In affected versions, a path traversal exists when processing a message in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution.</p>	<p><a href="https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640">https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640</a></p>	A-ROC-THIN-050423/1021

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
			<b>CVE ID : CVE-2023-27855</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	7.5	In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed.  <b>CVE ID : CVE-2023-27856</b>	<a href="https://rockwellautomation.com/answers/answer_view/a_id/1138640">https://rockwellautomation.com/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1022
Out-of-bounds Read	22-Mar-2023	7.5	In affected versions, a heap-based buffer over-read condition occurs when the message field indicates more data than is present in the message field in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to crash ThinServer.exe due to a read access violation.  <b>CVE ID : CVE-2023-27857</b>	<a href="https://rockwellautomation.com/answers/answer_view/a_id/1138640">https://rockwellautomation.com/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1023
Affected Version(s): 13.0.1					

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 Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	9.8	In affected versions, a path traversal exists when processing a message in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution.  <b>CVE ID : CVE-2023-27855</b>	<a href="https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640">https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1024
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	7.5	In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed.  <b>CVE ID : CVE-2023-27856</b>	<a href="https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640">https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1025

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): From (including) 11.0.0 Up to (excluding) 11.0.5					
Out-of-bounds Read	22-Mar-2023	7.5	In affected versions, a heap-based buffer over-read condition occurs when the message field indicates more data than is present in the message field in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to crash ThinServer.exe due to a read access violation.  <b>CVE ID : CVE-2023-27857</b>	<a href="https://rockwellautomation.com/answers/answer_view/a_id/1138640">https://rockwellautomation.com/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1026
Affected Version(s): From (including) 11.0.0 Up to (including) 11.0.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	9.8	In affected versions, a path traversal exists when processing a message in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious	<a href="https://rockwellautomation.com/answers/answer_view/a_id/1138640">https://rockwellautomation.com/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1027

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
			contents, potentially causing remote code execution. <b>CVE ID : CVE-2023-27855</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	7.5	In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed. <b>CVE ID : CVE-2023-27856</b>	<a href="https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640">https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1028
Affected Version(s): From (including) 11.1.0 Up to (excluding) 11.1.5					
Out-of-bounds Read	22-Mar-2023	7.5	In affected versions, a heap-based buffer over-read condition occurs when the message field indicates more data than is present in the message field in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to crash ThinServer.exe due to	<a href="https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640">https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1029

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
			a read access violation. <b>CVE ID : CVE-2023-27857</b>		
Affected Version(s): From (including) 11.1.0 Up to (including) 11.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	9.8	In affected versions, a path traversal exists when processing a message in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution. <b>CVE ID : CVE-2023-27855</b>	<a href="https://rockwellautomation.com/answers/answer_view/a_id/1138640">https://rockwellautomation.com/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1030
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	7.5	In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to	<a href="https://rockwellautomation.com/answers/answer_view/a_id/1138640">https://rockwellautomation.com/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1031

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
			download arbitrary files on the disk drive where ThinServer.exe is installed. <b>CVE ID : CVE-2023-27856</b>		
Affected Version(s): From (including) 11.2.0 Up to (excluding) 11.2.6					
Out-of-bounds Read	22-Mar-2023	7.5	In affected versions, a heap-based buffer over-read condition occurs when the message field indicates more data than is present in the message field in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to crash ThinServer.exe due to a read access violation. <b>CVE ID : CVE-2023-27857</b>	<a href="https://rockwellautomation.com/answers/answer_view/a_id/1138640">https://rockwellautomation.com/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1032
Affected Version(s): From (including) 11.2.0 Up to (including) 11.2.6					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	9.8	In affected versions, a path traversal exists when processing a message in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the	<a href="https://rockwellautomation.com/answers/answer_view/a_id/1138640">https://rockwellautomation.com/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1033

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
			<p>disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution.</p> <p><b>CVE ID : CVE-2023-27855</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	7.5	<p>In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed.</p> <p><b>CVE ID : CVE-2023-27856</b></p>	<p><a href="https://rockwellautomation.com/support/answers/answer_view/a_id/1138640">https://rockwellautomation.com/support/answers/answer_view/a_id/1138640</a></p>	A-ROC-THIN-050423/1034
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.0.3					
Out-of-bounds Read	22-Mar-2023	7.5	<p>In affected versions, a heap-based buffer over-read condition occurs when the message field indicates more data than is present in the message field in Rockwell Automation's ThinManager</p>	<p><a href="https://rockwellautomation.com/support/answers/answer_view/a_id/1138640">https://rockwellautomation.com/support/answers/answer_view/a_id/1138640</a></p>	A-ROC-THIN-050423/1035

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
			ThinServer. An unauthenticated remote attacker can exploit this vulnerability to crash ThinServer.exe due to a read access violation. <b>CVE ID : CVE-2023-27857</b>		
Affected Version(s): From (including) 12.0.0 Up to (including) 12.0.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	9.8	In affected versions, a path traversal exists when processing a message in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution. <b>CVE ID : CVE-2023-27855</b>	<a href="https://rockwellautomation.com/answers/answer_view/a_id/1138640">https://rockwellautomation.com/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1036
Improper Limitation of a Pathname to a Restricted	22-Mar-2023	7.5	In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's	<a href="https://rockwellautomation.com/answers/answer_vi">https://rockwellautomation.com/answers/answer_vi</a>	A-ROC-THIN-050423/1037

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed.  <b>CVE ID : CVE-2023-27856</b>	ew/a_id/1138640	
Affected Version(s): From (including) 12.1.0 Up to (excluding) 12.1.4					
Out-of-bounds Read	22-Mar-2023	7.5	In affected versions, a heap-based buffer over-read condition occurs when the message field indicates more data than is present in the message field in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to crash ThinServer.exe due to a read access violation.  <b>CVE ID : CVE-2023-27857</b>	<a href="https://rockwellautomation.com/answers/answer_view/a_id/1138640">https://rockwellautomation.com/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1038
Affected Version(s): From (including) 12.1.0 Up to (including) 12.1.5					
Improper Limitation of a Pathname to a Restricted Directory	22-Mar-2023	9.8	In affected versions, a path traversal exists when processing a message in Rockwell Automation's ThinManager ThinServer. An	<a href="https://rockwellautomation.com/answers/answer_view/a_id/1138640">https://rockwellautomation.com/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1039

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
('Path Traversal')			unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution.  <b>CVE ID : CVE-2023-27855</b>	ew/a_id/1138640	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	7.5	In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed.  <b>CVE ID : CVE-2023-27856</b>	<a href="https://rockwellautomation.com/answers/answer_view/a_id/1138640">https://rockwellautomation.com/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1040
Affected Version(s): From (including) 6.0.0 Up to (including) 10.0.2					
Improper Limitation of a Pathname to a	22-Mar-2023	9.8	In affected versions, a path traversal exists when processing a message in Rockwell Automation's	<a href="https://rockwellautomation.com/answers">https://rockwellautomation.com/answers</a>	A-ROC-THIN-050423/1041

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
Restricted Directory ('Path Traversal')			ThinManager ThinServer. An unauthenticated remote attacker could potentially exploit this vulnerability to upload arbitrary files to any directory on the disk drive where ThinServer.exe is installed. The attacker could overwrite existing executable files with attacker-controlled, malicious contents, potentially causing remote code execution.  <b>CVE ID : CVE-2023-27855</b>	/answer_view/a_id/1138640	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Mar-2023	7.5	In affected versions, path traversal exists when processing a message of type 8 in Rockwell Automation's ThinManager ThinServer. An unauthenticated remote attacker can exploit this vulnerability to download arbitrary files on the disk drive where ThinServer.exe is installed.  <b>CVE ID : CVE-2023-27856</b>	<a href="https://rockwellautomation.com/app/answers/answer_view/a_id/1138640">https://rockwellautomation.com/app/answers/answer_view/a_id/1138640</a>	A-ROC-THIN-050423/1042
<b>Vendor: ruifang-tech</b>					
<b>Product: rebuild</b>					
Affected Version(s): * Up to (including) 3.2.3					

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
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in Rebuild up to 3.2.3. Affected by this issue is some unknown functionality of the file /project/tasks/list. The manipulation leads to sql injection. 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-223742 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1610</b>	N/A	A-RUI-REBU-050423/1043
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in Rebuild up to 3.2.3. This affects an unknown part of the file /files/list-file. The manipulation leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The associated identifier of	<a href="https://github.com/getrebuild/rebuild/issues/598">https://github.com/getrebuild/rebuild/issues/598</a> , <a href="https://vuldb.com/?id.223743">https://vuldb.com/?id.223743</a> , <a href="https://vuldb.com/?ctid.223743">https://vuldb.com/?ctid.223743</a>	A-RUI-REBU-050423/1044

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
			this vulnerability is VDB-223743. <b>CVE ID : CVE-2023-1612</b>		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Mar-2023	8.8	A vulnerability classified as critical was found in Rebuild up to 3.2.3. Affected by this vulnerability is the function queryListOfConfig of the file /admin/robot/approval/list. The manipulation of the argument q leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The name of the patch is c9474f84e5f376dd2ade2078e3039961a9425da7. It is recommended to apply a patch to fix this issue. The identifier VDB-223381 was assigned to this vulnerability. <b>CVE ID : CVE-2023-1495</b>	<a href="https://github.com/getrebuild/rebuild/commit/c9474f84e5f376dd2ade2078e3039961a9425da7">https://github.com/getrebuild/rebuild/commit/c9474f84e5f376dd2ade2078e3039961a9425da7</a>	A-RUI-REBU-050423/1045
Improper Neutralization of Input During Web Page Generation	23-Mar-2023	6.1	A vulnerability has been found in Rebuild up to 3.2.3 and classified as problematic. This vulnerability affects unknown code of the file /feeds/post/publish.	N/A	A-RUI-REBU-050423/1046

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 Scripting')			The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-223744. <b>CVE ID : CVE-2023-1613</b>		
<b>Vendor: russh_project</b>					
<b>Product: russh</b>					
Affected Version(s): 0.37.0					
Improper Verification of Cryptographic Signature	16-Mar-2023	5.9	russh is a Rust SSH client and server library. Starting in version 0.34.0 and prior to versions 0.36.2 and 0.37.1, Diffie-Hellman key validation is insufficient, which can lead to insecure shared secrets and therefore breaks confidentiality. Connections between a russh client and server or those of a russh peer with some other misbehaving peer are most likely to be problematic. These may vulnerable to eavesdropping. Most other	<a href="https://github.com/warp-tech/russh/security/advisories/GHSA-cqvm-j2r2-hwpg">https://github.com/warp-tech/russh/security/advisories/GHSA-cqvm-j2r2-hwpg</a> , <a href="https://github.com/warp-tech/russh/commit/d831a3716d3719dc76f091fcea9d94bd4ef97c6e">https://github.com/warp-tech/russh/commit/d831a3716d3719dc76f091fcea9d94bd4ef97c6e</a>	A-RUS-RUSS-050423/1047

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
			implementations reject such keys, so this is mainly an interoperability issue in such a case. This issue is fixed in versions 0.36.2 and 0.37.1 <b>CVE ID : CVE-2023-28113</b>		
Affected Version(s): From (including) 0.34.0 Up to (excluding) 0.36.2					
Improper Verification of Cryptographic Signature	16-Mar-2023	5.9	russh is a Rust SSH client and server library. Starting in version 0.34.0 and prior to versions 0.36.2 and 0.37.1, Diffie-Hellman key validation is insufficient, which can lead to insecure shared secrets and therefore breaks confidentiality. Connections between a russh client and server or those of a russh peer with some other misbehaving peer are most likely to be problematic. These may vulnerable to eavesdropping. Most other implementations reject such keys, so this is mainly an interoperability issue in such a case. This issue is fixed in versions 0.36.2 and 0.37.1	<a href="https://github.com/arp-tech/russh/security/advisories/GHSA-cqvm-j2r2-hwpg">https://github.com/arp-tech/russh/security/advisories/GHSA-cqvm-j2r2-hwpg</a> , <a href="https://github.com/arp-tech/russh/commit/d831a3716d3719dc76f091fcea9d94bd4ef97c6e">https://github.com/arp-tech/russh/commit/d831a3716d3719dc76f091fcea9d94bd4ef97c6e</a>	A-RUS-RUSS-050423/1048

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
			<b>CVE ID : CVE-2023-28113</b>		
<b>Vendor: saan</b>					
<b>Product: world_clock</b>					
Affected Version(s): * Up to (including) 1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The Saan World Clock WordPress plugin through 1.8 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0145</b>	N/A	A-SAA-WORL-050423/1049
<b>Vendor: saml_project</b>					
<b>Product: saml</b>					
Affected Version(s): 0.4.12					
Allocation of Resources Without Limits or Throttling	22-Mar-2023	7.5	The crewjam/saml go library contains a partial implementation of the SAML standard in golang. Prior to version 0.4.13, the package's use of `flate.NewReader` does not limit the size of the input. The user can pass more than 1 MB of data in the HTTP request to the processing functions, which will be	<a href="https://github.com/crewjam/saml/commit/8e9236867d176ad6338c870a84e2039aef8a5021">https://github.com/crewjam/saml/commit/8e9236867d176ad6338c870a84e2039aef8a5021</a> , <a href="https://github.com/crewjam/saml/security/advisories/GHSA-">https://github.com/crewjam/saml/security/advisories/GHSA-</a>	A-SAM-SAML-050423/1050

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
			decompressed server-side using the Deflate algorithm. Therefore, after repeating the same request multiple times, it is possible to achieve a reliable crash since the operating system kills the process. This issue is patched in version 0.4.13. <b>CVE ID : CVE-2023-28119</b>	5mqj-xc49-246p	
<b>Vendor: Samsung</b>					
<b>Product: bixbytouch</b>					
Affected Version(s): * Up to (excluding) 3.2.02.5					
N/A	16-Mar-2023	5.5	Improper access control vulnerability in BixbyTouch prior to version 3.2.02.5 in China models allows untrusted applications access local files. <b>CVE ID : CVE-2023-21465</b>	<a href="https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03">https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03</a>	A-SAM-BIXB-050423/1051
<b>Product: calendar</b>					
Affected Version(s): * Up to (excluding) 12.3.08.2000					
N/A	16-Mar-2023	3.3	Improper access control in Samsung Calendar prior to versions 12.4.02.9000 in Android 13 and 12.3.08.2000 in Android 12 allows local attacker to configure improper status. <b>CVE ID : CVE-2023-21464</b>	<a href="https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03">https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03</a>	A-SAM-CALE-050423/1052

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): * Up to (excluding) 12.4.02.9000					
N/A	16-Mar-2023	3.3	Improper access control in Samsung Calendar prior to versions 12.4.02.9000 in Android 13 and 12.3.08.2000 in Android 12 allows local attacker to configure improper status.  <b>CVE ID : CVE-2023-21464</b>	<a href="https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03">https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03</a>	A-SAM-CALE-050423/1053
<b>Product: myfiles</b>					
Affected Version(s): * Up to (excluding) 12.2.09.0					
N/A	16-Mar-2023	3.3	Improper access control vulnerability in MyFiles application prior to versions 12.2.09.0 in Android 11, 13.1.03.501 in Android 12 and 14.1.03.0 in Android 13 allows local attacker to get sensitive information of secret mode in Samsung Internet application with specific conditions.  <b>CVE ID : CVE-2023-21463</b>	<a href="https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03">https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03</a>	A-SAM-MYFI-050423/1054
Affected Version(s): * Up to (excluding) 13.1.03.501					
N/A	16-Mar-2023	3.3	Improper access control vulnerability in MyFiles application prior to versions 12.2.09.0 in Android 11, 13.1.03.501 in Android 12 and 14.1.03.0 in Android	<a href="https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03">https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03</a>	A-SAM-MYFI-050423/1055

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
			13 allows local attacker to get sensitive information of secret mode in Samsung Internet application with specific conditions. <b>CVE ID : CVE-2023-21463</b>		
Affected Version(s): * Up to (excluding) 14.1.03.0					
N/A	16-Mar-2023	3.3	Improper access control vulnerability in MyFiles application prior to versions 12.2.09.0 in Android 11, 13.1.03.501 in Android 12 and 14.1.03.0 in Android 13 allows local attacker to get sensitive information of secret mode in Samsung Internet application with specific conditions. <b>CVE ID : CVE-2023-21463</b>	<a href="https://security.samsungmobile.com/service/Web.smsb?year=2023&amp;month=03">https://security.samsungmobile.com/service/Web.smsb?year=2023&amp;month=03</a>	A-SAM-MYFI-050423/1056
<b>Product: quick_share</b>					
Affected Version(s): * Up to (excluding) 3.5.14.18					
N/A	16-Mar-2023	3.3	The sensitive information exposure vulnerability in Quick Share Agent prior to versions 3.5.14.18 in Android 12 and 3.5.16.20 in Android 13 allows to local attacker to access MAC address without related permission.	<a href="https://security.samsungmobile.com/service/Web.smsb?year=2023&amp;month=03">https://security.samsungmobile.com/service/Web.smsb?year=2023&amp;month=03</a>	A-SAM-QUIC-050423/1057

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
			<b>CVE ID : CVE-2023-21462</b>		
Affected Version(s): * Up to (excluding) 3.5.16.20					
N/A	16-Mar-2023	3.3	The sensitive information exposure vulnerability in Quick Share Agent prior to versions 3.5.14.18 in Android 12 and 3.5.16.20 in Android 13 allows to local attacker to access MAC address without related permission. <b>CVE ID : CVE-2023-21462</b>	<a href="https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03">https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03</a>	A-SAM-QUIC-050423/1058
<b>Vendor: schedulicity</b>					
<b>Product: schedulicity</b>					
Affected Version(s): * Up to (including) 2.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	The Schedulicity WordPress plugin through 2.21 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0491</b>	N/A	A-SCH-SCHE-050423/1059
<b>Vendor: Schneider-electric</b>					
<b>Product: custom_reports</b>					
Affected Version(s): * Up to (including) 16.0.0.23040					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-Mar-2023	8.8	<p>A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior)</p> <p><b>CVE ID : CVE-2023-27980</b></p>	<p><a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a></p>	A-SCH-CUST-050423/1060
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Mar-2023	8.8	<p>A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoar</p>	<p><a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a></p>	A-SCH-CUST-050423/1061

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			d.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). <b>CVE ID : CVE-2023-27981</b>		
Insufficient Verification of Data Authenticity	21-Mar-2023	8.8	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(Dashboard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). <b>CVE ID : CVE-2023-27982</b>	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a>	A-SCH-CUST-050423/1062
Improper Input Validation	21-Mar-2023	8.8	A CWE-20: Improper Input Validation vulnerability exists in Custom Reports that	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a>	A-SCH-CUST-050423/1063

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
			could cause a macro to be executed, potentially leading to remote code execution when a user opens a malicious report file planted by an attacker. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). <b>CVE ID : CVE-2023-27984</b>	m/files?p_Doc_Ref=SEVD-2023-073-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	
Deserialization of Untrusted Data	21-Mar-2023	7.8	A CWE-502: Deserialization of Untrusted Data vulnerability exists in the Dashboard module that could cause an interpretation of malicious payload data, potentially leading to remote code execution when an attacker gets the user to open a malicious file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_enDocType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_enDocType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a>	A-SCH-CUST-050423/1064

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
			16.0.0.23040 and prior). <b>CVE ID : CVE-2023-27978</b>		
Insufficient Verification of Data Authenticity	21-Mar-2023	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause access to delete files in the IGSS project report directory, this could lead to loss of data when an attacker sends specific crafted messages to the Data Server TCP port. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). <b>CVE ID : CVE-2023-27977</b>	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a>	A-SCH-CUST-050423/1065
Insufficient Verification of Data Authenticity	21-Mar-2023	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could allow the renaming of files in the IGSS project report directory, this could lead to denial of	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+</a>	A-SCH-CUST-050423/1066

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
			<p>service when an attacker sends specific crafted messages to the Data Server TCP port. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).</p> <p><b>CVE ID : CVE-2023-27979</b></p>	Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	
Missing Authentication for Critical Function	21-Mar-2023	5.3	<p>A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow deletion of reports from the IGSS project report directory, this would lead to loss of data when an attacker abuses this functionality. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).</p> <p><b>CVE ID : CVE-2023-27983</b></p>	<p><a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_enDocType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_enDocType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a></p>	A-SCH-CUST-050423/1067

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
<b>Product: igss_dashboard</b>					
Affected Version(s): * Up to (including) 16.0.0.23040					
Missing Authentication for Critical Function	21-Mar-2023	8.8	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior) <b>CVE ID : CVE-2023-27980</b>	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a>	A-SCH-IGSS-050423/1068
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Mar-2023	8.8	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a malicious report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEV">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEV</a>	A-SCH-IGSS-050423/1069

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). <b>CVE ID : CVE-2023-27981</b>	D-2023-073-04.pdf	
Insufficient Verification of Data Authenticity	21-Mar-2023	8.8	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). <b>CVE ID : CVE-2023-27982</b>	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a>	A-SCH-IGSS-050423/1070

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 Input Validation	21-Mar-2023	8.8	A CWE-20: Improper Input Validation vulnerability exists in Custom Reports that could cause a macro to be executed, potentially leading to remote code execution when a user opens a malicious report file planted by an attacker. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). <b>CVE ID : CVE-2023-27984</b>	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_enDocType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_enDocType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a>	A-SCH-IGSS-050423/1071
Deserialization of Untrusted Data	21-Mar-2023	7.8	A CWE-502: Deserialization of Untrusted Data vulnerability exists in the Dashboard module that could cause an interpretation of malicious payload data, potentially leading to remote code execution when an attacker gets the user to open a malicious file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoar	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_enDocType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_enDocType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a>	A-SCH-IGSS-050423/1072

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
			<p>the IGSS project report directory, this could lead to denial of service when an attacker sends specific crafted messages to the Data Server TCP port. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).</p> <p><b>CVE ID : CVE-2023-27979</b></p>	<p>04&amp;p_enDo cType=Sec urity+and+ Safety+Noti ce&amp;p_File_ Name=SEV D-2023- 073-04.pdf</p>	
Missing Authentication for Critical Function	21-Mar-2023	5.3	<p>A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow deletion of reports from the IGSS project report directory, this would lead to loss of data when an attacker abuses this functionality. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V</p>	<p><a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_enDo&lt;br/&gt;cType=Sec&lt;br/&gt;urity+and+&lt;br/&gt;Safety+Noti&lt;br/&gt;ce&amp;p_File_&lt;br/&gt;Name=SEV&lt;br/&gt;D-2023-&lt;br/&gt;073-04.pdf">https://do wnload.sch neider- electric.co m/files?p_ Doc_Ref=SE VD-2023- 073- 04&amp;p_enDo cType=Sec urity+and+ Safety+Noti ce&amp;p_File_ Name=SEV D-2023- 073-04.pdf</a></p>	A-SCH-IGSS-050423/1075

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
			16.0.0.23040 and prior). <b>CVE ID : CVE-2023-27983</b>		
<b>Product: igss_data_server</b>					
Affected Version(s): * Up to (including) 16.0.0.23040					
Missing Authentication for Critical Function	21-Mar-2023	8.8	A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow the creation of a malicious report file in the IGSS project report directory, this could lead to remote code execution when a victim eventually opens the report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior) <b>CVE ID : CVE-2023-27980</b>	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a>	A-SCH-IGSS-050423/1076
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Mar-2023	8.8	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists in Custom Reports that could cause a remote code execution when a victim tries to open a	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endo">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endo</a>	A-SCH-IGSS-050423/1077

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
			malicious report. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). <b>CVE ID : CVE-2023-27981</b>	cType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	
Insufficient Verification of Data Authenticity	21-Mar-2023	8.8	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause manipulation of dashboard files in the IGSS project report directory, when an attacker sends specific crafted messages to the Data Server TCP port, this could lead to remote code execution when a victim eventually opens a malicious dashboard file. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endo cType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endo cType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a>	A-SCH-IGSS-050423/1078

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
			16.0.0.23040 and prior). <b>CVE ID : CVE-2023-27982</b>		
Improper Input Validation	21-Mar-2023	8.8	A CWE-20: Improper Input Validation vulnerability exists in Custom Reports that could cause a macro to be executed, potentially leading to remote code execution when a user opens a malicious report file planted by an attacker. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). <b>CVE ID : CVE-2023-27984</b>	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_enDocType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_enDocType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a>	A-SCH-IGSS-050423/1079
Deserialization of Untrusted Data	21-Mar-2023	7.8	A CWE-502: Deserialization of Untrusted Data vulnerability exists in the Dashboard module that could cause an interpretation of malicious payload data, potentially leading to remote code execution when an attacker gets the user to open a malicious file. Affected Products: IGSS Data	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_enDocType=Security+and+Safety+Notice&amp;p_File_Name=SEV">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_enDocType=Security+and+Safety+Notice&amp;p_File_Name=SEV</a>	A-SCH-IGSS-050423/1080

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
			Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(Dashboard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). <b>CVE ID : CVE-2023-27978</b>	D-2023-073-04.pdf	
Insufficient Verification of Data Authenticity	21-Mar-2023	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists in the Data Server that could cause access to delete files in the IGSS project report directory, this could lead to loss of data when an attacker sends specific crafted messages to the Data Server TCP port. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(Dashboard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). <b>CVE ID : CVE-2023-27977</b>	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a>	A-SCH-IGSS-050423/1081
Insufficient Verification of Data	21-Mar-2023	7.5	A CWE-345: Insufficient Verification of Data Authenticity	<a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endoctype=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a>	A-SCH-IGSS-050423/1082

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
Authenticity			<p>vulnerability exists in the Data Server that could allow the renaming of files in the IGSS project report directory, this could lead to denial of service when an attacker sends specific crafted messages to the Data Server TCP port. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoard.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior).</p> <p><b>CVE ID : CVE-2023-27979</b></p>	m/files?p_Doc_Ref=SEVD-2023-073-04&p_endOfcType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-04.pdf	
Missing Authentication for Critical Function	21-Mar-2023	5.3	<p>A CWE-306: Missing Authentication for Critical Function vulnerability exists in the Data Server TCP interface that could allow deletion of reports from the IGSS project report directory, this would lead to loss of data when an attacker abuses this functionality. Affected Products: IGSS Data Server(IGSSdataServer.exe)(V16.0.0.23040 and prior), IGSS Dashboard(DashBoar</p>	<p><a href="https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endOfcType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf">https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-04&amp;p_endOfcType=Security+and+Safety+Notice&amp;p_File_Name=SEVD-2023-073-04.pdf</a></p>	A-SCH-IGSS-050423/1083

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			d.exe)(V16.0.0.23040 and prior), Custom Reports(RMS16.dll)(V16.0.0.23040 and prior). <b>CVE ID : CVE-2023-27983</b>		

**Vendor: school\_registration\_and\_fee\_system\_project**

**Product: school\_registration\_and\_fee\_system**

Affected Version(s): 1.0

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Mar-2023	9.8	School Registration and Fee System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at/bilalfinal/edit_user.php. <b>CVE ID : CVE-2023-27041</b>	<a href="https://github.com/foersean/bug-report/blob/main/vendors/hemedy99/School%20Registration%20and%20Fee%20System/SQLi-1.md">https://github.com/foersean/bug-report/blob/main/vendors/hemedy99/School%20Registration%20and%20Fee%20System/SQLi-1.md</a>	A-SCH-SCHO-050423/1084
--	-------------	-----	---	---	------------------------

**Vendor: sentry**

**Product: sentry\_software\_development\_kit**

Affected Version(s): \* Up to (excluding) 1.14.0

Insertion of Sensitive Information Into Sent Data	22-Mar-2023	6.5	Sentry SDK is the official Python SDK for Sentry, real-time crash reporting software. When using the Django integration of versions prior to 1.14.0 of the Sentry SDK in a specific configuration it is possible to leak sensitive cookies values, including the session cookie to Sentry. These	<a href="https://github.com/getsentry/sentry-python/pull/1842">https://github.com/getsentry/sentry-python/pull/1842</a> , <a href="https://github.com/getsentry/sentry-python/security/advisories/GHSA-29pr-6jr8-q5jm">https://github.com/getsentry/sentry-python/security/advisories/GHSA-29pr-6jr8-q5jm</a>	A-SEN-SENT-050423/1085
---	-------------	-----	--	--	------------------------

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
			<p>sensitive cookies could then be used by someone with access to your Sentry issues to impersonate or escalate their privileges within your application. In order for these sensitive values to be leaked, the Sentry SDK configuration must have <code>`sendDefaultPII`</code> set to <code>`True`</code>; one must use a custom name for either <code>`SESSION_COOKIE_NAME`</code> or <code>`CSRF_COOKIE_NAME`</code> in one's Django settings; and one must not be configured in one's organization or project settings to use Sentry's data scrubbing features to account for the custom cookie names. As of version 1.14.0, the Django integration of the <code>`sentry-sdk`</code> will detect the custom cookie names based on one's Django settings and will remove the values from the payload before sending the data to Sentry. As a workaround, use the SDK's filtering mechanism to remove the cookies from the payload that is sent to</p>		

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
			<p>Sentry. For error events, this can be done with the `before_send` callback method and for performance related events (transactions) one can use the `before_send_transaction` callback method. Those who want to handle filtering of these values on the server-side can also use Sentry's advanced data scrubbing feature to account for the custom cookie names. Look for the `\$http.cookies`, `\$http.headers`, `\$request.cookies`, or `\$request.headers` fields to target with a scrubbing rule.</p> <p><b>CVE ID : CVE-2023-28117</b></p>		

**Vendor: service\_area\_postcode\_checker\_project**

**Product: service\_area\_postcode\_checker**

Affected Version(s): \* Up to (including) 2.0.8

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	4.8	<p>Auth. (admin+) vulnerability in Second2none Service Area Postcode Checker plugin &lt;= 2.0.8 versions.</p> <p><b>CVE ID : CVE-2023-25782</b></p>	N/A	A-SER-SERV-050423/1086
--	-------------	-----	---	-----	------------------------

**Vendor: silabs**

**Product: wi-sun\_software\_development\_kit**

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): * Up to (including) 1.5.0					
Missing Authorization	21-Mar-2023	5.3	Missing MAC layer security in Silicon Labs Wi-SUN SDK v1.5.0 and earlier allows malicious node to route malicious messages through network. <b>CVE ID : CVE-2023-1261</b>	N/A	A-SIL-WI-S-050423/1087
<b>Vendor: Silverstripe</b>					
<b>Product: graphql</b>					
Affected Version(s): 4.1.1					
Allocation of Resources Without Limits or Throttling	16-Mar-2023	7.5	`silverstripe/graphql` serves Silverstripe data as GraphQL representations. In versions 4.2.2 and 4.1.1, an attacker could use a specially crafted graphql query to execute a denial of service attack against a website which has a publicly exposed graphql endpoint. This mostly affects websites with particularly large/complex graphql schemas. Users should upgrade to `silverstripe/graphql` 4.2.3 or 4.1.2 to remedy the vulnerability. <b>CVE ID : CVE-2023-28104</b>	https://github.com/silverstripe/silverstripe-graphql/security/advisories/GHSA-67g8-c724-8mp3, https://github.com/silverstripe/silverstripe-graphql/releases/tag/4.1.2, https://github.com/silverstripe/silverstripe-graphql/pull/526	A-SIL-GRAP-050423/1088
Affected Version(s): 4.2.2					

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
Allocation of Resources Without Limits or Throttling	16-Mar-2023	7.5	<p>`silverstripe/graphql` serves Silverstripe data as GraphQL representations. In versions 4.2.2 and 4.1.1, an attacker could use a specially crafted graphql query to execute a denial of service attack against a website which has a publicly exposed graphql endpoint. This mostly affects websites with particularly large/complex graphql schemas. Users should upgrade to `silverstripe/graphql` 4.2.3 or 4.1.2 to remedy the vulnerability.</p> <p><b>CVE ID : CVE-2023-28104</b></p>	<p><a href="https://github.com/silverstripe/silverstripe-graphql/security/advisories/GHSA-67g8-c724-8mp3">https://github.com/silverstripe-graphql/security/advisories/GHSA-67g8-c724-8mp3</a>,  <a href="https://github.com/silverstripe/silverstripe-graphql/releases/tag/4.1.2">https://github.com/silverstripe/silverstripe-graphql/releases/tag/4.1.2</a>,  <a href="https://github.com/silverstripe/silverstripe-graphql/pull/526">https://github.com/silverstripe-graphql/pull/526</a></p>	A-SIL-GRAP-050423/1089

**Vendor: simplefilelist**

**Product: simple\_file\_list**

Affected Version(s): \* Up to (excluding) 6.0.10

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	4.8	<p>The Simple File List WordPress plugin before 6.0.10 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</p>	N/A	A-SIM-SIMP-050423/1090
--	-------------	-----	---	-----	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disallowed (for example in multisite setup). <b>CVE ID : CVE-2023-1025</b>		
<b>Vendor: simple_and_beautiful_shopping_cart_system_project</b>					
<b>Product: simple_and_beautiful_shopping_cart_system</b>					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	22-Mar-2023	9.8	A vulnerability classified as critical has been found in Simple and Beautiful Shopping Cart System 1.0. This affects an unknown part of the file uploadera.php. The manipulation 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-223551. <b>CVE ID : CVE-2023-1558</b>	N/A	A-SIM-SIMP-050423/1091
<b>Vendor: simple_and_nice_shopping_cart_script_project</b>					
<b>Product: simple_and_nice_shopping_cart_script</b>					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	19-Mar-2023	9.8	A vulnerability was found in SourceCodester Simple and Nice Shopping Cart Script 1.0. It has been rated as critical. This issue affects some unknown processing of the file	N/A	A-SIM-SIMP-050423/1092

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
			<p>uploaderm.php. The manipulation of the argument submit leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223397 was assigned to this vulnerability.</p> <p><b>CVE ID : CVE-2023-1497</b></p>		
<b>Vendor: simple_art_gallery_project</b>					
<b>Product: simple_art_gallery</b>					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Mar-2023	9.8	<p>A vulnerability classified as critical was found in code-projects Simple Art Gallery 1.0. Affected by this vulnerability is an unknown functionality of the file adminHome.php. The manipulation of the argument reach_city leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223399.</p> <p><b>CVE ID : CVE-2023-1499</b></p>	N/A	A-SIM-SIMP-050423/1093

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')	19-Mar-2023	6.1	A vulnerability, which was classified as problematic, has been found in code-projects Simple Art Gallery 1.0. Affected by this issue is some unknown functionality of the file adminHome.php. The manipulation of the argument about_info leads to cross site scripting. 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-223400.  <b>CVE ID : CVE-2023-1500</b>	N/A	A-SIM-SIMP-050423/1094
<b>Vendor: simple_customer_relationship_management_system_project</b>					
<b>Product: simple_customer_relationship_management_system</b>					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Mar-2023	9.8	Simple Customer Relationship Management System v1.0 was discovered to contain a SQL injection vulnerability via the name parameter under the Profile Update function.  <b>CVE ID : CVE-2023-24655</b>	N/A	A-SIM-SIMP-050423/1095
<b>Vendor: simple_image_gallery_web_app_project</b>					
<b>Product: simple_image_gallery_web_app</b>					
Affected Version(s): 1.0					

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 Special Elements in Output Used by a Downstream Component ('Injection')	16-Mar-2023	9.8	Simple Image Gallery v1.0 was discovered to contain a remote code execution (RCE) vulnerability via the username parameter. <b>CVE ID : CVE-2023-27040</b>	N/A	A-SIM-SIMP-050423/1096

**Vendor: simple\_music\_player\_project**

**Product: simple\_music\_player**

Affected Version(s): 1.0

Unrestricted Upload of File with Dangerous Type	18-Mar-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Simple Music Player 1.0. Affected is an unknown function of the file save_music.php. The manipulation of the argument filename 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-223362 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1479</b>	N/A	A-SIM-SIMP-050423/1097
---	-------------	-----	--	-----	------------------------

**Vendor: simple\_online\_hotel\_reservation\_system\_project**

**Product: simple\_online\_hotel\_reservation\_system**

Affected Version(s): 1.0

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
Unrestricted Upload of File with Dangerous Type	22-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in code-projects Simple Online Hotel Reservation System 1.0. Affected is an unknown function of the file add_room.php. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. VDB-223554 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1561</b>	N/A	A-SIM-SIMP-050423/1098

**Vendor: simplygallery**

**Product: simply\_gallery\_blocks\_with\_lightbox**

Affected Version(s): \* Up to (excluding) 3.0.8

Missing Authorization	27-Mar-2023	8.1	The Gallery Blocks with Lightbox WordPress plugin before 3.0.8 has an AJAX endpoint that can be accessed by any authenticated users, such as subscriber. The callback function allows numerous actions, the most serious one being reading and updating the WordPress options which could be used to enable registration with a default administrator user role.	N/A	A-SIM-SIMP-050423/1099
-----------------------	-------------	-----	--	-----	------------------------

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
			<b>CVE ID : CVE-2023-0441</b>		
<b>Vendor: smplredirectionsmanager_project</b>					
<b>Product: smplredirectionsmanager</b>					
Affected Version(s): * Up to (excluding) 1.1.19					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Mar-2023	9.8	SQL injection vulnerability found in PrestaShop smplredirectionsmanager v.1.1.19 and before allow a remote attacker to gain privileges via the SmplTools::getMatchingRedirectionsFromPartscomponent. <b>CVE ID : CVE-2023-26864</b>	<a href="https://friends-of-presta.github.io/security-advisories/modules/2023/01/17/smplredirectionsmanager.html">https://friends-of-presta.github.io/security-advisories/modules/2023/01/17/smplredirectionsmanager.html</a>	A-SMP-SMPL-050423/1100
<b>Vendor: softmaker</b>					
<b>Product: flexipdf</b>					
Affected Version(s): 2022					
Out-of-bounds Write	23-Mar-2023	7.8	A stack overflow in SoftMaker Software GmbH FlexiPDF v3.0.3.0 allows attackers to execute arbitrary code after opening a crafted PDF file. <b>CVE ID : CVE-2023-24295</b>	N/A	A-SOF-FLEX-050423/1101
<b>Vendor: squidex.io</b>					
<b>Product: squidex</b>					
Affected Version(s): * Up to (excluding) 7.4.0					
Improper Neutralization of Input During	18-Mar-2023	6.1	Squidex before 7.4.0 was discovered to contain a squid.svg cross-site scripting (XSS) vulnerability.	N/A	A-SQU-SQUI-050423/1102

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			<b>CVE ID : CVE-2023-24278</b>		
<b>Vendor: storage_unit_rental_management_system_project</b>					
<b>Product: storage_unit_rental_management_system</b>					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	22-Mar-2023	7.2	A vulnerability classified as problematic was found in SourceCodester Storage Unit Rental Management System 1.0. This vulnerability affects unknown code of the file classes/Users.php?f=save. The manipulation 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-223552. <b>CVE ID : CVE-2023-1559</b>	N/A	A-STO-STOR-050423/1103
<b>Vendor: strangerstudios</b>					
<b>Product: paid_memberships_pro</b>					
Affected Version(s): * Up to (excluding) 2.9.12					
Improper Neutralization of Special Elements used in an SQL Command	20-Mar-2023	8.8	The Paid Memberships Pro WordPress plugin before 2.9.12 does not prevent subscribers from rendering shortcodes that concatenate attributes	N/A	A-STR-PAID-050423/1104

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			directly into an SQL query. <b>CVE ID : CVE-2023-0631</b>		
<b>Vendor: strategy11</b>					
<b>Product: formidable_form_builder</b>					
Affected Version(s): * Up to (excluding) 6.1					
Authenticat ion Bypass by Spoofing	27-Mar-2023	6.5	The Formidable Forms WordPress plugin before 6.1 uses several potentially untrusted headers to determine the IP address of the client, leading to IP Address spoofing and bypass of anti-spam protections. <b>CVE ID : CVE-2023-0816</b>	N/A	A-STR-FORM-050423/1105
<b>Vendor: streamlit</b>					
<b>Product: streamlit</b>					
Affected Version(s): From (including) 0.63.0 Up to (excluding) 0.81.0					
Improper Neutralizat ion of Input During Web Page Generation ( <i>'Cross-site Scripting'</i> )	16-Mar-2023	6.1	Streamlit, software for turning data scripts into web applications, had a cross-site scripting (XSS) vulnerability in versions 0.63.0 through 0.80.0. Users of hosted Streamlit app(s) were vulnerable to a reflected XSS vulnerability. An attacker could craft a malicious URL with Javascript payloads to a Streamlit app. The attacker could then trick the user into	<a href="https://github.com/streamlit/streamlit/security/advisories/GHSA-9c6g-qpji-rvxw">https://github.com/streamlit/streamlit/security/advisories/GHSA-9c6g-qpji-rvxw</a> , <a href="https://github.com/streamlit/streamlit/commit/afcf880c60e5d7538936cc2d9721b9e1bc02b075">https://github.com/streamlit/streamlit/commit/afcf880c60e5d7538936cc2d9721b9e1bc02b075</a>	A-STR-STRE-050423/1106

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
			<p>visiting the malicious URL and, if successful, the server would render the malicious javascript payload as-is, leading to XSS.</p> <p>Version 0.81.0 contains a patch for this vulnerability.</p> <p><b>CVE ID : CVE-2023-27494</b></p>		
<b>Vendor: student_study_center_desk_management_system_project</b>					
<b>Product: student_study_center_desk_management_system</b>					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	<p>A vulnerability was found in SourceCodester Student Study Center Desk Management System 1.0. It has been rated as critical. This issue affects the function view_student of the file admin/?page=students/view_student. The manipulation of the argument id with the input 3' AND (SELECT 2100 FROM (SELECT(SLEEP(5))))FWIC) AND 'butz'='butz leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-223325 was assigned to this vulnerability.</p>	N/A	A-STU-STUD-050423/1107

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
			<b>CVE ID : CVE-2023-1466</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Mar-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Student Study Center Desk Management System 1.0. Affected is an unknown function of the file Master.php?f=delete_img of the component POST Parameter Handler. The manipulation of the argument path with the input C%3A%2Ffoo.txt leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-223326 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1467</b>	N/A	A-STU-STUD-050423/1108
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	9.8	A vulnerability classified as critical was found in SourceCodester Student Study Center Desk Management System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/?page=reports&date_from=2023-02-17&date_to=2023-03-	N/A	A-STU-STUD-050423/1109

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
			17 of the component Report Handler. The manipulation of the argument date_from/date_to leads to sql injection. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-223327. <b>CVE ID : CVE-2023-1468</b>		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	A vulnerability has been found in SourceCodester Student Study Center Desk Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/assign/assign.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223555. <b>CVE ID : CVE-2023-1563</b>	N/A	A-STU-STUD-050423/1110
Improper Neutralization of	22-Mar-2023	6.1	A vulnerability was found in SourceCodester	N/A	A-STU-STUD-050423/1111

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			<p>Student Study Center Desk Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/assign/assign.php. The manipulation of the argument sid 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-223559.</p> <p><b>CVE ID : CVE-2023-1567</b></p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	<p>A vulnerability classified as problematic has been found in SourceCodester Student Study Center Desk Management System 1.0. Affected is an unknown function of the file /admin/reports/index.php of the component GET Parameter Handler. The manipulation of the argument date_to leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to</p>	N/A	A-STU-STUD-050423/1112

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 public and may be used. The identifier of this vulnerability is VDB-223560. <b>CVE ID : CVE-2023-1568</b>		
<b>Vendor: sudo_project</b>					
<b>Product: sudo</b>					
Affected Version(s): * Up to (excluding) 1.9.13					
Improper Encoding or Escaping of Output	16-Mar-2023	5.3	Sudo before 1.9.13 does not escape control characters in log messages. <b>CVE ID : CVE-2023-28486</b>	<a href="https://github.com/sudo-project/sudo/commit/334daf92b31b79ce68ed75e2ee14fca265f029ca">https://github.com/sudo-project/sudo/commit/334daf92b31b79ce68ed75e2ee14fca265f029ca</a>	A-SUD-SUDO-050423/1113
Improper Encoding or Escaping of Output	16-Mar-2023	5.3	Sudo before 1.9.13 does not escape control characters in sudoreplay output. <b>CVE ID : CVE-2023-28487</b>	<a href="https://github.com/sudo-project/sudo/commit/334daf92b31b79ce68ed75e2ee14fca265f029ca">https://github.com/sudo-project/sudo/commit/334daf92b31b79ce68ed75e2ee14fca265f029ca</a>	A-SUD-SUDO-050423/1114
<b>Vendor: superior_faq_project</b>					
<b>Product: superior_faq</b>					
Affected Version(s): * Up to (including) 1.0.2					
Cross-Site Request Forgery (CSRF)	20-Mar-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Rafael Dery Superior FAQ plugin <= 1.0.2 versions. <b>CVE ID : CVE-2023-22678</b>	N/A	A-SUP-SUPE-050423/1115

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
<b>Vendor: Swftools</b>					
<b>Product: swftools</b>					
Affected Version(s): 0.9.2					
Out-of-bounds Write	23-Mar-2023	5.5	swfdump v0.9.2 was discovered to contain a heap buffer overflow in the function swf_GetPlaceObject at swfobject.c.  <b>CVE ID : CVE-2023-27249</b>	N/A	A-SWF-SWFT-050423/1116
<b>Vendor: tailscale</b>					
<b>Product: tailscale</b>					
Affected Version(s): From (including) 1.34 Up to (excluding) 1.38.2					
Improper Privilege Management	23-Mar-2023	8	Tailscale is software for using Wireguard and multi-factor authentication (MFA). A vulnerability identified in the implementation of Tailscale SSH starting in version 1.34.0 and prior to prior to 1.38.2 in FreeBSD allows commands to be run with a higher privilege group ID than that specified in Tailscale SSH access rules. A difference in the behavior of the FreeBSD `setgroups` system call from POSIX meant that the Tailscale client running on a FreeBSD-based operating system did not appropriately restrict groups on the host	<a href="https://github.com/tailscale/tailscale/releases/tag/v1.38.2">https://github.com/tailscale/tailscale/releases/tag/v1.38.2</a> , <a href="https://tailscale.com/security-bulletins/#ts-2023-003">https://tailscale.com/security-bulletins/#ts-2023-003</a> , <a href="https://github.com/tailscale/tailscale/commit/d00c046b723dff6e3775d7d35f891403ac21a47d">https://github.com/tailscale/tailscale/commit/d00c046b723dff6e3775d7d35f891403ac21a47d</a>	A-TAI-TAIL-050423/1117

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
			<p>when using Tailscale SSH. When accessing a FreeBSD host over Tailscale SSH, the egid of the tailscaled process was used instead of that of the user specified in Tailscale SSH access rules. Tailscale SSH commands may have been run with a higher privilege group ID than that specified in Tailscale SSH access rules if they met all of the following criteria: the destination node was a FreeBSD device with Tailscale SSH enabled; Tailscale SSH access rules permitted access for non-root users; and a non-interactive SSH session was used. Affected users should upgrade to version 1.38.2 to remediate the issue.</p> <p><b>CVE ID : CVE-2023-28436</b></p>		

**Vendor: task\_allocation\_system\_project**

**Product: task\_allocation\_system**

Affected Version(s): 1.0

Improper Neutralization of Input During Web Page Generation	29-Mar-2023	6.1	A vulnerability classified as problematic has been found in SourceCodester Simple Task Allocation System 1.0. Affected is	N/A	A-TAS-TASK-050423/1118
---	-------------	-----	---	-----	------------------------

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 Scripting')			an unknown function of the file LoginRegistration.php?a=register_user. The manipulation of the argument Fullname leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-224244.  <b>CVE ID : CVE-2023-1687</b>		
<b>Vendor: teachpress_project</b>					
<b>Product: teachpress</b>					
Affected Version(s): * Up to (excluding) 8.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Reflected Cross-Site Scripting (XSS) vulnerability in Michael Winkler teachPress plugin <= 8.1.8 versions.  <b>CVE ID : CVE-2023-22704</b>	N/A	A-TEA-TEAC-050423/1119
<b>Vendor: teacms_project</b>					
<b>Product: teacms</b>					
Affected Version(s): * Up to (including) 2.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Mar-2023	9.8	A vulnerability has been found in XiaoBingBy TeaCMS up to 2.0.2 and classified as critical. This vulnerability affects unknown code of the file /admin/getallarticleinfo. The manipulation of the argument	N/A	A-TEA-TEAC-050423/1120

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
			searchInfo leads to sql injection. The attack can be initiated remotely. VDB-223366 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1483</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Mar-2023	5.4	A vulnerability was found in XiaoBingBy TeaCMS up to 2.0.2. It has been classified as problematic. Affected is an unknown function of the component Article Title Handler. The manipulation with the input <code>&lt;script&gt;alert(document.cookie)&lt;/script&gt;</code> 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-223800. <b>CVE ID : CVE-2023-1616</b>	N/A	A-TEA-TEAC-050423/1121
<b>Vendor: Teampass</b>					
<b>Product: teampass</b>					
Affected Version(s): * Up to (excluding) 3.0.0.23					
Improper Neutralization of Special Elements used in an	21-Mar-2023	7.5	SQL Injection in GitHub repository nilsteampassnet/team pass prior to 3.0.0.23.	<a href="https://huntr.dev/bounties/942c015f-7486-49b1-94ae-">https://huntr.dev/bounties/942c015f-7486-49b1-94ae-</a>	A-TEA-TEAM-050423/1122

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			<b>CVE ID : CVE-2023-1545</b>	b1538d812bc2, <a href="https://github.com/nilsteampassnet/teampass/commit/4780252fdb600ef2ec2758f17a37d738570cbe66">https://github.com/nilsteampassnet/teampass/commit/4780252fdb600ef2ec2758f17a37d738570cbe66</a>	
Authorization Bypass Through User-Controlled Key	17-Mar-2023	5.4	Improper Authorization in GitHub repository nilsteampassnet/team pass prior to 3.0.0.23. <b>CVE ID : CVE-2023-1463</b>	<a href="https://huntr.dev/bounties/f6683c3b-a0f2-4615-b639-1920c8ae12e6">https://huntr.dev/bounties/f6683c3b-a0f2-4615-b639-1920c8ae12e6</a> , <a href="https://github.com/nilsteampassnet/teampass/commit/4e06fbaf2b78c3615d0599855a72ba7e31157516">https://github.com/nilsteampassnet/teampass/commit/4e06fbaf2b78c3615d0599855a72ba7e31157516</a>	A-TEA-TEAM-050423/1123
<b>Vendor: technocrackers</b>					
<b>Product: bulk_price_update_for_woocommerce</b>					
Affected Version(s): * Up to (excluding) 2.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	The Woo Bulk Price Update WordPress plugin, in versions < 2.2.2, is affected by a reflected cross-site scripting vulnerability in the 'page' parameter to the techno_get_products	N/A	A-TEC-BULK-050423/1124

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
			action, which can only be triggered by an authenticated user. <b>CVE ID : CVE-2023-28665</b>		
<b>Vendor: temenos</b>					
<b>Product: t24</b>					
Affected Version(s): r20					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	6.1	Temenos T24 Release 20 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the routineName parameter at genrequest.jsp. <b>CVE ID : CVE-2023-24367</b>	N/A	A-TEM-T24-050423/1125
<b>Vendor: templatesnext</b>					
<b>Product: templatesnext_toolkit</b>					
Affected Version(s): * Up to (excluding) 3.2.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in TemplatesNext Toolkit plugin <= 3.2.7 versions. <b>CVE ID : CVE-2023-22712</b>	N/A	A-TEM-TEMP-050423/1126
<b>Vendor: tinydng_project</b>					
<b>Product: tinydng</b>					
Affected Version(s): * Up to (excluding) 2023-02-20					
Heap-based Buffer Overflow	22-Mar-2023	5.5	A vulnerability, which was classified as problematic, has been found in syoyo tinydng. Affected by	<a href="https://github.com/syoyo/tinydng/issues/29">https://github.com/syoyo/tinydng/issues/29</a> ,	A-TIN-TINY-050423/1127

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
			<p>this issue is the function <code>_interceptor_memcpy</code> of the file <code>tiny_dng_loader.h</code>. The manipulation leads to heap-based buffer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. Continuous delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. It is recommended to apply a patch to fix this issue. VDB-223562 is the identifier assigned to this vulnerability.</p> <p><b>CVE ID : CVE-2023-1570</b></p>	<a href="https://github.com/yoyo/tinydng/issues/28">https://github.com/yoyo/tinydng/issues/28</a>	
<b>Vendor: tinytiff_project</b>					
<b>Product: tinytiff</b>					
Affected Version(s): 3.0.0.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Mar-2023	5.5	A vulnerability, which was classified as problematic, has been found in TinyTIFF 3.0.0.0. This issue affects some unknown processing of the file <code>tinytiffreader.c</code> of the component File Handler. The manipulation leads to	N/A	A-TIN-TINY-050423/1128

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
			<p>buffer overflow. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The identifier VDB-223553 was assigned to this vulnerability.</p> <p><b>CVE ID : CVE-2023-1560</b></p>		
<b>Vendor: Tipsandtricks-hq</b>					
<b>Product: wordpress_simple_paypal_shopping_cart</b>					
Affected Version(s): * Up to (including) 4.6.3					
Exposure of Sensitive Information to an Unauthorized Actor	16-Mar-2023	5.3	<p>The WP Simple Shopping Cart plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 4.6.3 due to the plugin saving shopping cart data exports in a publicly accessible location (/wp-content/plugins/wordpress-simple-paypal-shopping-cart/includes/admin/). This makes it possible for unauthenticated attackers to view information that should be limited to administrators only and can include data like first name, last name, email, address, IP Address, and more.</p>	N/A	A-TIP-WORD-050423/1129

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
			<b>CVE ID : CVE-2023-1431</b>		
<b>Product: wp_express_checkout</b>					
Affected Version(s): * Up to (excluding) 2.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Mar-2023	4.8	The WP Express Checkout plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pec_coupon[code]' parameter in versions up to, and including, 2.2.8 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. Note: This can potentially be exploited by lower-privileged users if the 'Admin Dashboard Access Permission' setting is set for those users to access the dashboard.  <b>CVE ID : CVE-2023-1469</b>	<a href="https://plugins.trac.wordpress.org/changest?sf_email=&amp;sfph_mail=&amp;reponame=&amp;old=2879453%40wp-express-checkout&amp;new=2879453%40wp-express-checkout&amp;sf_email=&amp;sfph_mail=">https://plugins.trac.wordpress.org/changest?sf_email=&amp;sfph_mail=&amp;reponame=&amp;old=2879453%40wp-express-checkout&amp;new=2879453%40wp-express-checkout&amp;sf_email=&amp;sfph_mail=</a>	A-TIP-WP_E-050423/1130
<b>Vendor: top_10_-_popular_posts_project</b>					
<b>Product: top_10_-_popular_posts</b>					
Affected Version(s): * Up to (including) 3.2.4					

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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Ajay D'Souza Top 10 – Popular posts plugin for WordPress plugin <= 3.2.4 versions. <b>CVE ID : CVE-2023-26008</b>	N/A	A-TOP-TOP_-050423/1131
<b>Vendor: tosec</b>					
<b>Product: kirin_fortress_machine</b>					
Affected Version(s): 1.7-2020-0610					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Mar-2023	9.8	SQL Injection vulnerability found in Kirin Fortress Machine v.1.7-2020-0610 allows attackers to execute arbitrary code via the /admin.php?controller=admin_commonuser parameter. <b>CVE ID : CVE-2023-26784</b>	N/A	A-TOS-KIRI-050423/1132
<b>Vendor: Trendmicro</b>					
<b>Product: trend_micro_endpoint_encryption</b>					
Affected Version(s): * Up to (including) 6.0.0.3204					
N/A	22-Mar-2023	6.8	A vulnerability in Trend Micro Endpoint Encryption Full Disk Encryption version 6.0.0.3204 and below could allow an attacker with physical access to an affected device to bypass Microsoft Windows? Secure Boot process in an attempt to execute other attacks to obtain access to the contents	<a href="https://success.trendmicro.com/solution/000292473">https://success.trendmicro.com/solution/000292473</a>	A-TRE-TREN-050423/1133

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
			<p>of the device. An attacker must first obtain physical access to the target system in order to exploit this vulnerability. It is also important to note that the contents of the drive(s) encrypted with TMEE FDE would still be protected and would NOT be accessible by the attacker by exploitation of this vulnerability alone.</p> <p><b>CVE ID : CVE-2023-28005</b></p>		

**Product: txone\_stellarone**

Affected Version(s): \* Up to (excluding) 2.0.1160

N/A	22-Mar-2023	8.8	<p>TXOne StellarOne has an improper access control privilege escalation vulnerability in every version before V2.0.1160 that could allow a malicious, falsely authenticated user to escalate his privileges to administrator level. With these privileges, an attacker could perform actions they are not authorized to. Please note: an attacker must first obtain a low-privileged authenticated user's profile on the target system in order to</p>	<p><a href="https://success.trendmicro.com/solution/000292486">https://success.trendmicro.com/solution/000292486</a></p>	A-TRE-TXON-050423/1134
-----	-------------	-----	--	--	------------------------

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
			exploit this vulnerability. <b>CVE ID : CVE-2023-25069</b>		
<b>Vendor: tribe29</b>					
<b>Product: checkmk</b>					
Affected Version(s): 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	HTML Email Injection in Tribe29 Checkmk <=2.1.0p23; <=2.0.0p34, and all versions of Checkmk 1.6.0 allows an authenticated attacker to inject malicious HTML into Emails <b>CVE ID : CVE-2023-22288</b>	<a href="https://checkmk.com/werk/15069">https://checkmk.com/werk/15069</a>	A-TRI-CHEC-050423/1135
Affected Version(s): 2.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	HTML Email Injection in Tribe29 Checkmk <=2.1.0p23; <=2.0.0p34, and all versions of Checkmk 1.6.0 allows an authenticated attacker to inject malicious HTML into Emails <b>CVE ID : CVE-2023-22288</b>	<a href="https://checkmk.com/werk/15069">https://checkmk.com/werk/15069</a>	A-TRI-CHEC-050423/1136
Affected Version(s): From (including) 1.6.0 Up to (excluding) 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	HTML Email Injection in Tribe29 Checkmk <=2.1.0p23; <=2.0.0p34, and all versions of Checkmk 1.6.0 allows an authenticated attacker to inject malicious HTML into Emails	<a href="https://checkmk.com/werk/15069">https://checkmk.com/werk/15069</a>	A-TRI-CHEC-050423/1137

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
			<b>CVE ID : CVE-2023-22288</b>		
<b>Vendor: trudesk_project</b>					
<b>Product: trudesk</b>					
Affected Version(s): 1.2.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Mar-2023	5.4	Trudesk v1.2.6 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Add Tags parameter under the Create Ticket function. <b>CVE ID : CVE-2023-26982</b>	N/A	A-TRU-TRUD-050423/1138
<b>Vendor: tshirtecommerce</b>					
<b>Product: tshirtecommerce</b>					
Affected Version(s): 2.1.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	An issue was discovered in the tshirtecommerce (aka Custom Product Designer) component 2.1.4 for PrestaShop. An HTTP request can be forged with a compromised product_id GET parameter in order to exploit an insecure parameter in the front controller file designer.php, which could lead to a SQL injection. This is exploited in the wild in March 2023. <b>CVE ID : CVE-2023-27637</b>	<a href="https://friends-of-presta.github.io/security-advisories/module/2023/03/21/tshirtecommerce_cwe-89.html">https://friends-of-presta.github.io/security-advisories/module/2023/03/21/tshirtecommerce_cwe-89.html</a>	A-TSH-TSHI-050423/1139

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Mar-2023	9.8	An issue was discovered in the tshirtecommerce (aka Custom Product Designer) component 2.1.4 for PrestaShop. An HTTP request can be forged with a compromised tshirtecommerce_design_cart_id GET parameter in order to exploit an insecure parameter in the functions hookActionCartSave and updateCustomization Table, which could lead to a SQL injection. This is exploited in the wild in March 2023. <b>CVE ID : CVE-2023-27638</b>	<a href="https://friends-of-presta.github.io/security-advisories/module/2023/03/21/tshirtecommerce_cwe-89.html">https://friends-of-presta.github.io/security-advisories/module/2023/03/21/tshirtecommerce_cwe-89.html</a>	A-TSH-TSHI-050423/1140
<b>Vendor: typecho</b>					
<b>Product: typecho</b>					
Affected Version(s): * Up to (including) 1.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-2023	4.8	Cross Site Scripting vulnerability found in Typecho v.1.2.0 allows a remote attacker to execute arbitrary code via an arbitrarily supplied URL parameter. <b>CVE ID : CVE-2023-27130</b>	<a href="https://github.com/typecho/typecho/commit/f9ede542c9052ba22a6096d8412e2f02d9de872b">https://github.com/typecho/typecho/commit/f9ede542c9052ba22a6096d8412e2f02d9de872b</a>	A-TYP-TYPE-050423/1141
Improper Neutralization of Input During	16-Mar-2023	4.8	Cross Site Scripting vulnerability found in Typecho v.1.2.0 allows a remote attacker to execute arbitrary code	N/A	A-TYP-TYPE-050423/1142

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			via the Post Editor parameter. <b>CVE ID : CVE-2023-27131</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Mar-2023	4.8	Cross Site Scripting vulnerability found in Typecho v.1.2.0 allows a remote attacker to execute arbitrary code via the Comment Manager /admin/manage-comments.php component. <b>CVE ID : CVE-2023-27711</b>	N/A	A-TYP-TYPE-050423/1143
<b>Vendor: university_information_management_system_project</b>					
<b>Product: university_information_management_system</b>					
Affected Version(s): * Up to (excluding) 23.03.16					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Izmir Katip Celebi University UBYS allows Stored XSS. This issue affects UBYS: before 23.03.16. <b>CVE ID : CVE-2023-0320</b>	N/A	A-UNI-UNIV-050423/1144
<b>Vendor: utarit</b>					
<b>Product: persolus</b>					
Affected Version(s): * Up to (excluding) 2.03.93					
Improper Neutralization of Special Elements	17-Mar-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	N/A	A-UTA-PERS-050423/1145

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			vulnerability in Utarit Information Technologies Persolus allows SQL Injection. This issue affects Persolus: before 2.03.93. <b>CVE ID : CVE-2023-1152</b>		
<b>Vendor: vadi</b>					
<b>Product: digikent</b>					
Affected Version(s): * Up to (excluding) 23.03.20					
Authorizati on Bypass Through User-Controlled Key	21-Mar-2023	8.8	Authorization Bypass Through User-Controlled Key vulnerability in Vadi Corporate Information Systems DigiKent allows Authentication Bypass, Authentication Abuse. This issue affects DigiKent: before 23.03.20. <b>CVE ID : CVE-2023-1462</b>	N/A	A-VAD-DIGI-050423/1146
<b>Vendor: vektor-inc</b>					
<b>Product: vk_all_in_one_expansion_unit</b>					
Affected Version(s): * Up to (excluding) 9.87.1.0					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	6.1	The VK All in One Expansion Unit WordPress plugin before 9.87.1.0 does not escape the \$_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which could lead to Reflected Cross-Site	N/A	A-VEK-VK_A-050423/1147

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
			Scripting in old web browsers <b>CVE ID : CVE-2023-0937</b>		
<b>Vendor: Veritas</b>					
<b>Product: aptare_it_analytics</b>					
Affected Version(s): * Up to (excluding) 10.6.00					
Improper Verification of Cryptographic Signature	24-Mar-2023	5.3	An issue was discovered in Veritas NetBackup IT Analytics 11 before 11.2.0. The application upgrade process included unsigned files that could be exploited and result in a customer installing unauthentic components. A malicious actor could install rogue Collector executable files (aptare.jar or upgrademanager.zip) on the Portal server, which might then be downloaded and installed on collectors. <b>CVE ID : CVE-2023-28818</b>	<a href="https://www.veritas.com/content/support/en_US/security/VTS23-002">https://www.veritas.com/content/support/en_US/security/VTS23-002</a>	A-VER-APTA-050423/1148
<b>Product: netbackup</b>					
Affected Version(s): * Up to (excluding) 10.0					
Uncontrolled Search Path Element	23-Mar-2023	7.8	An issue was discovered in Veritas NetBackup before 10.0. A vulnerability in the way NetBackup validates the path to a DLL prior to loading may allow a lower level user to elevate	<a href="https://www.veritas.com/content/support/en_US/security/VTS22-010#M2">https://www.veritas.com/content/support/en_US/security/VTS22-010#M2</a>	A-VER-NETB-050423/1149

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
			privileges and compromise the system. <b>CVE ID : CVE-2023-28759</b>		
Affected Version(s): * Up to (excluding) 8.3.0.2					
N/A	23-Mar-2023	7.1	An issue was discovered in Veritas NetBackup before 8.3.0.2. BPCD allows an unprivileged user to specify a log file path when executing a NetBackup command. This can be used to overwrite existing NetBackup log files. <b>CVE ID : CVE-2023-28758</b>	<a href="https://www.veritas.com/content/support/en_US/security/VTS23-003">https://www.veritas.com/content/support/en_US/security/VTS23-003</a>	A-VER-NETB-050423/1150
<b>Product: netbackup_it_analytics</b>					
Affected Version(s): 11.0.00					
Improper Verification of Cryptographic Signature	24-Mar-2023	5.3	An issue was discovered in Veritas NetBackup IT Analytics 11 before 11.2.0. The application upgrade process included unsigned files that could be exploited and result in a customer installing unauthentic components. A malicious actor could install rogue Collector executable files (aptare.jar or upgrademanager.zip) on the Portal server, which might then be	<a href="https://www.veritas.com/content/support/en_US/security/VTS23-002">https://www.veritas.com/content/support/en_US/security/VTS23-002</a>	A-VER-NETB-050423/1151

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
			downloaded and installed on collectors. <b>CVE ID : CVE-2023-28818</b>		
Affected Version(s): 11.1.00					
Improper Verification of Cryptographic Signature	24-Mar-2023	5.3	An issue was discovered in Veritas NetBackup IT Analytics 11 before 11.2.0. The application upgrade process included unsigned files that could be exploited and result in a customer installing unauthentic components. A malicious actor could install rogue Collector executable files (aptare.jar or upgrademanager.zip) on the Portal server, which might then be downloaded and installed on collectors. <b>CVE ID : CVE-2023-28818</b>	<a href="https://www.veritas.com/content/support/en_US/security/VTS23-002">https://www.veritas.com/content/support/en_US/security/VTS23-002</a>	A-VER-NETB-050423/1152
<b>Vendor: veronalabs</b>					
<b>Product: wp_statistics</b>					
Affected Version(s): * Up to (excluding) 14.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Mar-2023	8.8	The WP Statistics WordPress plugin before 14.0 does not escape a parameter, which could allow authenticated users to perform SQL Injection attacks. By default, the affected feature is available to users with	N/A	A-VER-WP_S-050423/1153

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
			<p>the manage_options capability (admin+), however the plugin has a settings to allow low privilege users to access it as well.</p> <p><b>CVE ID : CVE-2023-0955</b></p>		
<b>Vendor: versionize_project</b>					
<b>Product: versionize</b>					
Affected Version(s): From (including) 0.1.1 Up to (excluding) 0.1.10					
Out-of-bounds Read	24-Mar-2023	7.5	<p>Versionize is a framework for version tolerant serialization/deserialization of Rust data structures, designed for usecases that need fast deserialization times and minimal size overhead. An issue was discovered in the 'Versionize::deserialize' implementation provided by the 'versionize' crate for 'vmm_sys_utils::fam::FamStructWrapper', which can lead to out of bounds memory accesses. The impact started with version 0.1.1. The issue was corrected in version 0.1.10 by inserting a check that verifies, for any deserialized header, the lengths of compared flexible arrays are equal and aborting</p>	<p><a href="https://github.com/firecracker-microvm/versionize/commit/a57a051ba006cfa3b41a0532f484df759e008d47">https://github.com/firecracker-microvm/versionize/commit/a57a051ba006cfa3b41a0532f484df759e008d47</a></p>	A-VER-VERS-050423/1154

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
			deserialization otherwise. <b>CVE ID : CVE-2023-28448</b>		
<b>Vendor: very_simple_google_maps_project</b>					
<b>Product: very_simple_google_maps</b>					
Affected Version(s): * Up to (excluding) 2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Michael Aronoff Very Simple Google Maps plugin <= 2.8.4 versions. <b>CVE ID : CVE-2023-23864</b>	N/A	A-VER-VERY-050423/1155
<b>Vendor: VMware</b>					
<b>Product: spring_cloud_config</b>					
Affected Version(s): From (including) 3.1.0 Up to (including) 3.1.6					
Insertion of Sensitive Information into Log File	23-Mar-2023	5.5	In Spring Vault, versions 3.0.x prior to 3.0.2 and versions 2.3.x prior to 2.3.3 and older versions, an application is vulnerable to insertion of sensitive information into a log file when it attempts to revoke a Vault batch token. <b>CVE ID : CVE-2023-20859</b>	<a href="https://spring.io/security/cve-2023-20859">https://spring.io/security/cve-2023-20859</a>	A-VMW-SPRI-050423/1156
Affected Version(s): From (including) 4.0.0 Up to (including) 4.0.1					
Insertion of Sensitive Information into Log File	23-Mar-2023	5.5	In Spring Vault, versions 3.0.x prior to 3.0.2 and versions 2.3.x prior to 2.3.3 and older versions, an	<a href="https://spring.io/security/cve-2023-20859">https://spring.io/security/cve-2023-20859</a>	A-VMW-SPRI-050423/1157

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
			<p>application is vulnerable to insertion of sensitive information into a log file when it attempts to revoke a Vault batch token.</p> <p><b>CVE ID : CVE-2023-20859</b></p>		
<b>Product: spring_cloud_vault</b>					
Affected Version(s): 4.0.0					
Insertion of Sensitive Information into Log File	23-Mar-2023	5.5	<p>In Spring Vault, versions 3.0.x prior to 3.0.2 and versions 2.3.x prior to 2.3.3 and older versions, an application is vulnerable to insertion of sensitive information into a log file when it attempts to revoke a Vault batch token.</p> <p><b>CVE ID : CVE-2023-20859</b></p>	<a href="https://spring.io/security/cve-2023-20859">https://spring.io/security/cve-2023-20859</a>	A-VMW-SPRI-050423/1158
Affected Version(s): From (including) 3.1.0 Up to (including) 3.1.2					
Insertion of Sensitive Information into Log File	23-Mar-2023	5.5	<p>In Spring Vault, versions 3.0.x prior to 3.0.2 and versions 2.3.x prior to 2.3.3 and older versions, an application is vulnerable to insertion of sensitive information into a log file when it attempts to revoke a Vault batch token.</p> <p><b>CVE ID : CVE-2023-20859</b></p>	<a href="https://spring.io/security/cve-2023-20859">https://spring.io/security/cve-2023-20859</a>	A-VMW-SPRI-050423/1159
<b>Product: spring_framework</b>					

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): * Up to (including) 5.2.22					
N/A	23-Mar-2023	6.5	In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.  <b>CVE ID : CVE-2023-20861</b>	<a href="https://spring.io/security/cve-2023-20861">https://spring.io/security/cve-2023-20861</a>	A-VMW-SPRI-050423/1160
Affected Version(s): From (including) 5.3.0 Up to (including) 5.3.25					
N/A	23-Mar-2023	6.5	In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.  <b>CVE ID : CVE-2023-20861</b>	<a href="https://spring.io/security/cve-2023-20861">https://spring.io/security/cve-2023-20861</a>	A-VMW-SPRI-050423/1161
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.6					
N/A	23-Mar-2023	6.5	In Spring Framework versions 6.0.0 - 6.0.6, 5.3.0 - 5.3.25, 5.2.0.RELEASE - 5.2.22.RELEASE, and older unsupported versions, it is possible for a user to provide a specially crafted SpEL	<a href="https://spring.io/security/cve-2023-20861">https://spring.io/security/cve-2023-20861</a>	A-VMW-SPRI-050423/1162

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
			expression that may cause a denial-of-service (DoS) condition. <b>CVE ID : CVE-2023-20861</b>		
<b>Product: spring_vault</b>					
Affected Version(s): From (including) 2.3.0 Up to (excluding) 2.3.3					
Insertion of Sensitive Information into Log File	23-Mar-2023	5.5	In Spring Vault, versions 3.0.x prior to 3.0.2 and versions 2.3.x prior to 2.3.3 and older versions, an application is vulnerable to insertion of sensitive information into a log file when it attempts to revoke a Vault batch token. <b>CVE ID : CVE-2023-20859</b>	<a href="https://spring.io/security/cve-2023-20859">https://spring.io/security/cve-2023-20859</a>	A-VMW-SPRI-050423/1163
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.2					
Insertion of Sensitive Information into Log File	23-Mar-2023	5.5	In Spring Vault, versions 3.0.x prior to 3.0.2 and versions 2.3.x prior to 2.3.3 and older versions, an application is vulnerable to insertion of sensitive information into a log file when it attempts to revoke a Vault batch token. <b>CVE ID : CVE-2023-20859</b>	<a href="https://spring.io/security/cve-2023-20859">https://spring.io/security/cve-2023-20859</a>	A-VMW-SPRI-050423/1164
<b>Vendor: vox2mesh_project</b>					
<b>Product: vox2mesh</b>					
Affected Version(s): 1.0					

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
Out-of-bounds Write	22-Mar-2023	5.5	<p>vox2mesh 1.0 has stack-overflow in main.cpp, this is stack-overflow caused by incorrect use of memcopy() funciton. The flow allows an attacker to cause a denial of service (abort) via a crafted file.</p> <p><b>CVE ID : CVE-2023-27754</b></p>	N/A	A-VOX-VOX2-050423/1165
<b>Vendor: vxsearch</b>					
<b>Product: vx_search</b>					
Affected Version(s): 13.8					
Unquoted Search Path or Element	16-Mar-2023	7.8	<p>VX Search v13.8 and v14.7 was discovered to contain an unquoted service path vulnerability which allows attackers to execute arbitrary commands at elevated privileges via a crafted executable file.</p> <p><b>CVE ID : CVE-2023-24671</b></p>	N/A	A-VXS-VX_S-050423/1166
Affected Version(s): 14.7					
Unquoted Search Path or Element	16-Mar-2023	7.8	<p>VX Search v13.8 and v14.7 was discovered to contain an unquoted service path vulnerability which allows attackers to execute arbitrary commands at elevated privileges via a crafted executable file.</p> <p><b>CVE ID : CVE-2023-24671</b></p>	N/A	A-VXS-VX_S-050423/1167

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
<b>Vendor: watchdog</b>					
<b>Product: anti-virus</b>					
Affected Version(s): 1.4.214.0					
Improper Access Control	17-Mar-2023	7.1	A vulnerability was found in Watchdog Anti-Virus 1.4.214.0. It has been rated as critical. Affected by this issue is the function 0x80002008 in the library wsdk-driver.sys of the component IoControlCode Handler. The manipulation leads to improper access controls. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. VDB-223298 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1453</b>	N/A	A-WAT-ANTI-050423/1168
NULL Pointer Dereference	17-Mar-2023	5.5	A vulnerability classified as problematic was found in Watchdog Anti-Virus 1.4.214.0. Affected by this vulnerability is the function 0x80002004/0x80002008 in the library wsdk-driver.sys of the component IoControlCode Handler. The	N/A	A-WAT-ANTI-050423/1169

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
			manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223291. <b>CVE ID : CVE-2023-1446</b>		
<b>Vendor: water_billing_system_project</b>					
<b>Product: water_billing_system</b>					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	SourceCodester Water Billing System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the lastname text box under the Add Client module. <b>CVE ID : CVE-2023-27241</b>	<a href="https://github.com/kaikai-11/WaterBilling-System">https://github.com/kaikai-11/WaterBilling-System</a> , <a href="https://github.com/kaikai-11/WaterBilling-System/blob/main/README.md">https://github.com/kaikai-11/WaterBilling-System/blob/main/README.md</a>	A-WAT-WATE-050423/1170
<b>Vendor: webnus</b>					
<b>Product: modern_events_calendar_lite</b>					
Affected Version(s): * Up to (including) 5.16.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	4.8	The Modern Events Calendar Lite WordPress plugin through 5.16.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to	N/A	A-WEB-MODE-050423/1171

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
			perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). <b>CVE ID : CVE-2023-1400</b>		
<b>Vendor: westerndigital</b>					
<b>Product: sandisk_privateaccess</b>					
Affected Version(s): * Up to (excluding) 6.4.9					
Use of a Broken or Risky Cryptographic Algorithm	24-Mar-2023	7.4	SanDisk PrivateAccess versions prior to 6.4.9 support insecure TLS 1.0 and TLS 1.1 protocols which are susceptible to man-in-the-middle attacks thereby compromising confidentiality and integrity of data. <b>CVE ID : CVE-2023-22812</b>	<a href="https://www.westerndigital.com/support/product-security/wdc-23005-sandisk-privateaccess-software-update">https://www.westerndigital.com/support/product-security/wdc-23005-sandisk-privateaccess-software-update</a>	A-WES-SAND-050423/1172
<b>Vendor: winwar</b>					
<b>Product: wp_ ebay_product_feeds</b>					
Affected Version(s): * Up to (excluding) 3.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Winwar Media WP eBay Product Feeds plugin <= 3.3.1 versions. <b>CVE ID : CVE-2023-23722</b>	N/A	A-WIN-WP_E-050423/1173
<b>Product: wp_flipclock</b>					
Affected Version(s): * Up to (excluding) 1.8					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Winwar Media WP Flipclock plugin <= 1.7.4 versions. <b>CVE ID : CVE-2023-23728</b>	N/A	A-WIN-WP_F-050423/1174
<b>Vendor: wisdomgarden</b>					
<b>Product: tronclass_ilearn</b>					
Affected Version(s): 2.3.2					
Unrestricted Upload of File with Dangerous Type	27-Mar-2023	6.5	WisdomGarden Tronclass has improper access control when uploading file. An authenticated remote attacker with general user privilege can exploit this vulnerability to access files belonging to other users by modifying the file ID within URL. <b>CVE ID : CVE-2023-24834</b>	<a href="https://www.twcert.org.tw/tw/cp-132-6954-ed16b-1.html">https://www.twcert.org.tw/tw/cp-132-6954-ed16b-1.html</a>	A-WIS-TRON-050423/1175
Affected Version(s): * Up to (excluding) 1.52.29198					
Unrestricted Upload of File with Dangerous Type	27-Mar-2023	6.5	WisdomGarden Tronclass has improper access control when uploading file. An authenticated remote attacker with general user privilege can exploit this vulnerability to access files belonging to other users by	<a href="https://www.twcert.org.tw/tw/cp-132-6954-ed16b-1.html">https://www.twcert.org.tw/tw/cp-132-6954-ed16b-1.html</a>	A-WIS-TRON-050423/1176

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
			modifying the file ID within URL. <b>CVE ID : CVE-2023-24834</b>		
<b>Vendor: wisecleaner</b>					
<b>Product: wise_force_deleter</b>					
Affected Version(s): 1.5.3.54					
Improper Access Control	18-Mar-2023	7.1	A vulnerability classified as problematic was found in Lespeed WiseCleaner Wise Force Deleter 1.5.3.54. This vulnerability affects the function 0x220004 in the library WiseUnlock64.sys of the component IoControlCode Handler. The manipulation leads to improper access controls. 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 VDB-223372. <b>CVE ID : CVE-2023-1486</b>	N/A	A-WIS-WISE-050423/1177
<b>Product: wise_system_monitor</b>					
Affected Version(s): 1.5.3.54					
Improper Access Control	18-Mar-2023	7.8	A vulnerability has been found in Lespeed WiseCleaner Wise System Monitor 1.5.3.54 and classified	N/A	A-WIS-WISE-050423/1178

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
			<p>as critical. Affected by this vulnerability is the function 0x9C402088 in the library WiseHDInfo64.dll of the component IoControlCode Handler. The manipulation leads to improper access controls. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223375.</p> <p><b>CVE ID : CVE-2023-1489</b></p>		
Improper Resource Shutdown or Release	18-Mar-2023	5.5	<p>A vulnerability, which was classified as problematic, has been found in Lespeed WiseCleaner Wise System Monitor 1.5.3.54. This issue affects the function 0x9C40208C/0x9C402000/0x9C402084/0x9C402088/0x9C402004/0x9C4060C4/0x9C4060CC/0x9C4060D0/0x9C4060D4/0x9C40A0DC/0x9C40A0D8/0x9C40A0DC/0x9C40A0E0 in the library WiseHDInfo64.dll of the component IoControlCode Handler. The</p>	N/A	A-WIS-WISE-050423/1179

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
			manipulation leads to denial of service. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The identifier VDB-223373 was assigned to this vulnerability. <b>CVE ID : CVE-2023-1487</b>		
Improper Resource Shutdown or Release	18-Mar-2023	5.5	A vulnerability, which was classified as problematic, was found in Lespeed WiseCleaner Wise System Monitor 1.5.3.54. Affected is the function 0x9C40A0D8/0x9C40A0DC/0x9C40A0E0 in the library WiseHDInfo64.dll of the component IoControlCode Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. VDB-223374 is the identifier assigned to this vulnerability. <b>CVE ID : CVE-2023-1488</b>	N/A	A-WIS-WISE-050423/1180
<b>Vendor: woocommerce_multiple_customer_addresses_&amp;_shipping_project</b>					
<b>Product: woocommerce_multiple_customer_addresses_&amp;_shipping</b>					
Affected Version(s): * Up to (excluding) 21.7					

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
Authorization Bypass Through User-Controlled Key	20-Mar-2023	8.8	The WooCommerce Multiple Customer Addresses & Shipping WordPress plugin before 21.7 does not ensure that the address to add/update/retrieve/delete and duplicate belong to the user making the request, or is from a high privilege users, allowing any authenticated users, such as subscriber to add/update/duplicate/delete as well as retrieve addresses of other users.  <b>CVE ID : CVE-2023-0865</b>	N/A	A-WOO-WOOC-050423/1181
<b>Vendor: wp-commentnavi_project</b>					
<b>Product: wp-commentnavi</b>					
Affected Version(s): * Up to (excluding) 1.12.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	4.8	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Lester 'GaMerZ' Chan WP-CommentNavi plugin <= 1.12.1 versions.  <b>CVE ID : CVE-2023-22715</b>	N/A	A-WP--WP-C-050423/1182
<b>Vendor: wp-master</b>					
<b>Product: feed_changer_&amp;_remove</b>					
Affected Version(s): * Up to (including) 0.2					
Improper Neutralization of Input	20-Mar-2023	4.8	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in WP-master.Ir Feed	N/A	A-WP--FEED-050423/1183

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Changer & Remover plugin <= 0.2 versions. <b>CVE ID : CVE-2023-25795</b>		
<b>Vendor: wp-slimstat</b>					
<b>Product: slimstat_analytics</b>					
Affected Version(s): * Up to (excluding) 4.9.3.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Mar-2023	8.8	The Slimstat Analytics WordPress plugin before 4.9.3.3 does not prevent subscribers from rendering shortcodes that concatenates attributes directly into an SQL query. <b>CVE ID : CVE-2023-0630</b>	N/A	A-WP--SLIM-050423/1184
<b>Vendor: wpbean</b>					
<b>Product: wpb_advanced_faq</b>					
Affected Version(s): * Up to (excluding) 1.06					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	5.4	The WPB Advanced FAQ WordPress plugin through 1.0.6 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0370</b>	N/A	A-WPB-WPB_-050423/1185
<b>Vendor: wpmobile.app_project</b>					

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
<b>Product: wpmobile.app</b>					
Affected Version(s): * Up to (excluding) 11.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Mar-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in WPMobile.App WPMobile.App — Android and iOS Mobile Application plugin <= 11.13 versions. <b>CVE ID : CVE-2023-22702</b>	N/A	A-WPM-WPMO-050423/1186
<b>Vendor: wppool</b>					
<b>Product: wp_dark_mode</b>					
Affected Version(s): * Up to (excluding) 4.0.8					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Mar-2023	4.3	The WP Dark Mode WordPress plugin before 4.0.8 does not properly sanitize the style parameter in shortcodes before using it to load a PHP template. This leads to Local File Inclusion on servers where non-existent directories may be traversed, or when chained with another vulnerability allowing arbitrary directory creation. <b>CVE ID : CVE-2023-0467</b>	N/A	A-WPP-WP_D-050423/1187
<b>Vendor: wppvar</b>					
<b>Product: wp_shamsi</b>					
Affected Version(s): * Up to (including) 4.3.3					
Cross-Site Request	27-Mar-2023	6.5	The WP Shamsi WordPress plugin through 4.3.3 has	N/A	A-WPV-WP_S-050423/1188

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
Forgery (CSRF)			CSRF and broken access control vulnerabilities which leads user with role as low as subscriber delete attachment. <b>CVE ID : CVE-2023-0335</b>		
<b>Vendor: wp_better_emails_project</b>					
<b>Product: wp_better_emails</b>					
Affected Version(s): * Up to (including) 0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Nicolas Lemoine WP Better Emails plugin <= 0.4 versions. <b>CVE ID : CVE-2023-22679</b>	N/A	A-WP_-WP_B-050423/1189
<b>Vendor: wp_htpasswd_project</b>					
<b>Product: wp_htpasswd</b>					
Affected Version(s): * Up to (including) 1.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Mar-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Matteo Candura WP htpasswd plugin <= 1.7 versions. <b>CVE ID : CVE-2023-25064</b>	N/A	A-WP_-WP_H-050423/1190
<b>Vendor: wp_image_carousel_project</b>					
<b>Product: wp_image_carousel</b>					
Affected Version(s): * Up to (including) 1.0.2					
Improper Neutralization of Input	27-Mar-2023	5.4	The WP Image Carousel WordPress plugin through 1.0.2 does not sanitise and	N/A	A-WP_-WP_I-050423/1191

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			escape some parameters, which could allow users with a role as low as contributor to perform Cross-Site Scripting attacks. <b>CVE ID : CVE-2023-0589</b>		
<b>Vendor: wp_popup_banners_project</b>					
<b>Product: wp_popup_banners</b>					
Affected Version(s): * Up to (including) 1.2.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Mar-2023	6.5	The WP Popup Banners plugin for WordPress is vulnerable to SQL Injection via the 'banner_id' parameter in versions up to, and including, 1.2.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with minimal permissions, such as a subscriber, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. <b>CVE ID : CVE-2023-1471</b>	N/A	A-WP_-WP_P-050423/1192
<b>Vendor: X.org</b>					
<b>Product: x_server</b>					

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): * Up to (excluding) 21.1.7					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/003320.html">https://lists.x.org/archives/xorg-announce/2023-February/003320.html</a>	A-X.O-X_SE-050423/1193
<b>Vendor: xipblog_project</b>					
<b>Product: xipblog</b>					
Affected Version(s): * Up to (including) 2.0.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Mar-2023	9.8	SQL injection vulnerability found in PrestaShop xipblog v.2.0.1 and before allow a remote attacker to gain privileges via the xipcategoryclass and xippostsclass components. <b>CVE ID : CVE-2023-27847</b>	N/A	A-XIP-XIPB-050423/1194
<b>Vendor: xpdfreader</b>					
<b>Product: xpdf</b>					
Affected Version(s): 4.04					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.5	xpdf v4.04 was discovered to contain a stack overflow in the component pdftotext. <b>CVE ID : CVE-2023-27655</b>	<a href="https://for um.xpdfreader.com/viewtopic.php?t=42398">https://for um.xpdfreader.com/viewtopic.php?t=42398</a>	A-XPD-XPDF-050423/1195
<b>Vendor: xuxueli</b>					
<b>Product: xxl-job</b>					
Affected Version(s): 2.2.0					
N/A	21-Mar-2023	7.5	Permissions vulnerabilitiy found in Xuxueli xxl-job v2.2.0, v 2.3.0 and v.2.3.1 allows attacker to obtain sensitive information via the pageList parameter. <b>CVE ID : CVE-2023-27087</b>	N/A	A-XUX-XXL--050423/1196
Affected Version(s): 2.3.0					
N/A	21-Mar-2023	7.5	Permissions vulnerabilitiy found in Xuxueli xxl-job v2.2.0, v 2.3.0 and v.2.3.1 allows attacker to obtain sensitive information via the pageList parameter. <b>CVE ID : CVE-2023-27087</b>	N/A	A-XUX-XXL--050423/1197
Affected Version(s): 2.3.1					
N/A	21-Mar-2023	7.5	Permissions vulnerabilitiy found in Xuxueli xxl-job v2.2.0, v 2.3.0 and v.2.3.1 allows attacker to obtain sensitive information via the pageList parameter.	N/A	A-XUX-XXL--050423/1198

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
			<b>CVE ID : CVE-2023-27087</b>		
<b>Vendor: xzjie cms project</b>					
<b>Product: xzjie cms</b>					
Affected Version(s): * Up to (including) 1.0.3					
Unrestricted Upload of File with Dangerous Type	18-Mar-2023	9.8	A vulnerability was found in xzjie cms up to 1.0.3 and classified as critical. This issue affects some unknown processing of the file /api/upload. The manipulation of the argument uploadFile leads to unrestricted upload. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-223367.  <b>CVE ID : CVE-2023-1484</b>	<a href="https://github.com/xzjie/cms/issues/16INIT">https://github.com/xzjie/cms/issues/16INIT</a>	A-XZJ-XZJI-050423/1199
<b>Vendor: young_entrepreneur_e-negosyo_system_project</b>					
<b>Product: young_entrepreneur_e-negosyo_system</b>					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Mar-2023	6.1	A vulnerability classified as problematic has been found in SourceCodester Young Entrepreneur E-Negosyo System 1.0. This affects an unknown part of the file /bsenordering/index.php of the component GET Parameter Handler. The manipulation of the	N/A	A-YOU-YOUN-050423/1200

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
			<p>argument category with the input <code>&lt;script&gt;alert(222)&lt;/script&gt;</code> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223371.</p> <p><b>CVE ID : CVE-2023-1485</b></p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Mar-2023	6.1	<p>A vulnerability was found in SourceCodester Young Entrepreneur E-Negosyo System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file <code>bsenordering/admin/category/index.php</code> of the component GET Parameter Handler. The manipulation of the argument <code>view</code> with the input <code>&lt;script&gt;alert(233)&lt;/script&gt;</code> 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-224243.</p>	N/A	A-YOU-YOUN-050423/1201

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
			<b>CVE ID : CVE-2023-1686</b>		
<b>Vendor: Zoom</b>					
<b>Product: meetings</b>					
Affected Version(s): * Up to (excluding) 5.13.5					
N/A	16-Mar-2023	7.8	Zoom Client for IT Admin Windows installers before version 5.13.5 contain a local privilege escalation vulnerability. A local low-privileged user could exploit this vulnerability in an attack chain during the installation process to escalate their privileges to the SYSTEM user. <b>CVE ID : CVE-2023-22883</b>	<a href="https://explores.zoom.us/en/trust/security/security-bulletin/">https://explores.zoom.us/en/trust/security/security-bulletin/</a>	A-ZOO-MEET-050423/1202
<b>Product: rooms</b>					
Affected Version(s): * Up to (excluding) 5.13.3					
N/A	16-Mar-2023	7.5	Zoom for Windows clients before version 5.13.3, Zoom Rooms for Windows clients before version 5.13.5 and Zoom VDI for Windows clients before 5.13.1 contain an information disclosure vulnerability. A recent update to the Microsoft Edge WebView2 runtime used by the affected Zoom clients, transmitted text to	<a href="https://explores.zoom.us/en/trust/security/security-bulletin/">https://explores.zoom.us/en/trust/security/security-bulletin/</a>	A-ZOO-ROOM-050423/1203

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
			<p>Microsoft's online Spellcheck service instead of the local Windows Spellcheck. Updating Zoom remediates this vulnerability by disabling the feature. Updating Microsoft Edge WebView2 Runtime to at least version 109.0.1481.0 and restarting Zoom remediates this vulnerability by updating Microsoft's telemetry behavior.</p> <p><b>CVE ID : CVE-2023-22880</b></p>		
<b>Product: virtual_desktop_infrastructure</b>					
Affected Version(s): * Up to (excluding) 5.13.1					
N/A	16-Mar-2023	7.5	<p>Zoom for Windows clients before version 5.13.3, Zoom Rooms for Windows clients before version 5.13.5 and Zoom VDI for Windows clients before 5.13.1 contain an information disclosure vulnerability. A recent update to the Microsoft Edge WebView2 runtime used by the affected Zoom clients, transmitted text to Microsoft's online Spellcheck service instead of the local Windows Spellcheck. Updating Zoom</p>	<p><a href="https://explore.zoom.us/en/trust/security/security-bulletin/">https://explore.zoom.us/en/trust/security/security-bulletin/</a></p>	A-ZOO-VIRT-050423/1204

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
			remediates this vulnerability by disabling the feature. Updating Microsoft Edge WebView2 Runtime to at least version 109.0.1481.0 and restarting Zoom remediates this vulnerability by updating Microsoft's telemetry behavior. <b>CVE ID : CVE-2023-22880</b>		
<b>Product: zoom</b>					
Affected Version(s): * Up to (excluding) 5.13.5					
N/A	16-Mar-2023	7.5	Zoom clients before version 5.13.5 contain a STUN parsing vulnerability. A malicious actor could send specially crafted UDP traffic to a victim Zoom client to remotely cause the client to crash, causing a denial of service. <b>CVE ID : CVE-2023-22881</b>	<a href="https://explore.zoom.us/en/trust/security/security-bulletin/">https://explore.zoom.us/en/trust/security/security-bulletin/</a>	A-ZOO-ZOOM-050423/1205
N/A	16-Mar-2023	7.5	Zoom clients before version 5.13.5 contain a STUN parsing vulnerability. A malicious actor could send specially crafted UDP traffic to a victim Zoom client to remotely cause the client to crash, causing a denial of service.	<a href="https://explore.zoom.us/en/trust/security/security-bulletin/">https://explore.zoom.us/en/trust/security/security-bulletin/</a>	A-ZOO-ZOOM-050423/1206

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
			<b>CVE ID : CVE-2023-22882</b>		
Affected Version(s): * Up to (excluding) 5.13.3					
N/A	16-Mar-2023	7.5	<p>Zoom for Windows clients before version 5.13.3, Zoom Rooms for Windows clients before version 5.13.5 and Zoom VDI for Windows clients before 5.13.1 contain an information disclosure vulnerability. A recent update to the Microsoft Edge WebView2 runtime used by the affected Zoom clients, transmitted text to Microsoft's online Spellcheck service instead of the local Windows Spellcheck. Updating Zoom remediates this vulnerability by disabling the feature. Updating Microsoft Edge WebView2 Runtime to at least version 109.0.1481.0 and restarting Zoom remediates this vulnerability by updating Microsoft's telemetry behavior.</p> <p><b>CVE ID : CVE-2023-22880</b></p>	<p><a href="https://explore.zoom.us/en/trust/security/security-bulletin/">https://explore.zoom.us/en/trust/security/security-bulletin/</a></p>	A-ZOO-ZOOM-050423/1207
<b>Hardware</b>					
<b>Vendor: 360</b>					
<b>Product: d901</b>					

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): -					
Out-of-bounds Write	23-Mar-2023	7.5	Stack Overflow vulnerability found in 360 D901 allows a remote attacker to cause a Distributed Denial of Service (DDOS) via a crafted HTTP package. <b>CVE ID : CVE-2023-27077</b>	N/A	H-360-D901-050423/1208
<b>Vendor: centralite</b>					
<b>Product: pearl</b>					
Affected Version(s): -					
N/A	17-Mar-2023	7.5	A vulnerability in Centralite Pearl Thermostat 0x04075010 allows attackers to cause a Denial of Service (DoS) via a crafted Zigbee message. <b>CVE ID : CVE-2023-24678</b>	N/A	H-CEN-PEAR-050423/1209
<b>Vendor: Cisco</b>					
<b>Product: 8101-32fh</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-8101-050423/1210

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
			<p>escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-8101-050423/1211

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-8101-050423/1212
<b>Product: 8101-32h</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-8101-050423/1213

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-8101-050423/1214</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-8101-050423/1215

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: 8102-64h</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-8102-050423/1216
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-8102-050423/1217

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-8102-050423/1218

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: 8201**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-8201-050423/1219
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-8201-050423/1220
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-8201-050423/1221

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: 8201-32fh</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-8201-050423/1222

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-8201-050423/1223

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-8201-050423/1224
<b>Product: 8202</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-8202-050423/1225

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-8202-050423/1226</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-8202-050423/1227

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: 8800_12-slot</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-8800-050423/1228
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-8800-050423/1229

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-8800-050423/1230

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: 8800\_18-slot**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-8800-050423/1231
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-8800-050423/1232
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-8800-050423/1233

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: 8800_4-slot</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-8800-050423/1234

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-8800-050423/1235

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-8800-050423/1236
<b>Product: 8800_8-slot</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-8800-050423/1237

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-8800-050423/1238</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-8800-050423/1239

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: 8804</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-8804-050423/1240
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-8804-050423/1241

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-8804-050423/1242

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: 8808**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-8808-050423/1243
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-8808-050423/1244
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-8808-050423/1245

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: 8812</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-8812-050423/1246

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-8812-050423/1247

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-8812-050423/1248
<b>Product: 8818</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-8818-050423/1249

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-8818-050423/1250</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-8818-050423/1251

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: 8831</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-8831-050423/1252
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-8831-050423/1253

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-8831-050423/1254

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: 9800-40**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-9800-050423/1255
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V</a>	H-CIS-9800-050423/1256
<b>Product: 9800-80</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a>	H-CIS-9800-050423/1257

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
			<p>affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-9800-050423/1258

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
			UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
<b>Product: 9800-cl</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-9800-050423/1259
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-9800-050423/1260

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
<b>Product: 9800-l</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-9800-050423/1261

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
			commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-9800-050423/1262
<b>Product: aironet_1540</b>					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	H-CIS-AIRO-050423/1263

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: aironet\_1542d**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-AIRO-050423/1264
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: aironet\_1542i**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-AIRO-050423/1265
-----	-------------	-----	---	---	------------------------

**Product: aironet\_1560**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-AIRO-050423/1266
-----	-------------	-----	--	---	------------------------

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: aironet\_1562d**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-AIRO-050423/1267
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: aironet\_1562e**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-AIRO-050423/1268
-----	-------------	-----	---	---	------------------------

**Product: aironet\_1562i**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-AIRO-050423/1269
-----	-------------	-----	--	---	------------------------

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: aironet\_1800**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-AIRO-050423/1270
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: aironet\_1800i**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-AIRO-050423/1271
-----	-------------	-----	---	---	------------------------

**Product: aironet\_1810**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-AIRO-050423/1272
-----	-------------	-----	--	---	------------------------

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: aironet\_1810w**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-AIRO-050423/1273
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: aironet\_1815**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-AIRO-050423/1274
-----	-------------	-----	---	---	------------------------

**Product: aironet\_1815i**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	H-CIS-AIRO-050423/1275
-----	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: aironet\_1815m**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-AIRO-050423/1276
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: aironet\_1815t**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-AIRO-050423/1277
-----	-------------	-----	---	---	------------------------

**Product: aironet\_1815w**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-AIRO-050423/1278
-----	-------------	-----	--	---	------------------------

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: aironet\_2800**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-AIRO-050423/1279
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: aironet\_2800e**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-AIRO-050423/1280
-----	-------------	-----	---	---	------------------------

**Product: aironet\_2800i**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-AIRO-050423/1281
-----	-------------	-----	--	---	------------------------

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: aironet\_3800**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-AIRO-050423/1282
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: aironet\_3800e**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-AIRO-050423/1283
-----	-------------	-----	---	---	------------------------

**Product: aironet\_3800i**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	H-CIS-AIRO-050423/1284
-----	-------------	-----	--	---	------------------------

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: aironet\_3800p**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-AIRO-050423/1285
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: aironet\_4800**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-AIRO-050423/1286
-----	-------------	-----	---	---	------------------------

**Product: asr\_1000**

Affected Version(s): -

N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	H-CIS-ASR_-050423/1287
-----	-------------	-----	---	---	------------------------

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
			<p>could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	<p>H-CIS-ASR_-050423/1288</p>

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
			<p>UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1289

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
			man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: asr_1000-esp100</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1290
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-</a>	H-CIS-ASR_-050423/1291

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
			<p>due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1292

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
			<p>device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: asr_1000-esp100-x</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1293

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1294
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ASR_-050423/1295

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: asr_1000-esp200-x</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR-050423/1296

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ASR_-050423/1297

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1298
<b>Product: asr_1000-x</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ASR_-050423/1299
<b>Product: asr_1001</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-ASR_-050423/1300

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-ASR_-050423/1301</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1302

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: asr_1001-hx</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1303
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-ASR_-050423/1304

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1305

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: asr\_1001-hx\_r**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1306
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1307
<b>Product: asr_1001-x</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a>	H-CIS-ASR_-050423/1308

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
			<p>insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	ios-xe-sdwan-VQAhEjYw	
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1309

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
			<p>this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ASR_-050423/1310

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ASR_-050423/1311
<b>Product: asr_1001-x_r</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-ASR_-050423/1312

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-ASR_-050423/1313</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1314

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: asr_1002</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1315
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-ASR_-050423/1316

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1317

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: asr\_1002-hx**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhejYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhejYw</a></p>	H-CIS-ASR_-050423/1318
-----	-------------	-----	---	--	------------------------

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
			<p>system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>		
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1319
Improper Limitation of a Pathname	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote</p>	<p><a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a></p>	H-CIS-ASR_-050423/1320

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			<p>attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	ter/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1321

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
			<p>validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: asr\_1002-hx\_r**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1322
-----	-------------	-----	--	--	------------------------

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
			commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1323
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor</a>	H-CIS-ASR_-050423/1324

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
			<p>Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	y/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	

**Product: asr\_1002-x**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-iox-priv-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-iox-priv-</a></p>	H-CIS-ASR_-050423/1325
-----	-------------	-----	---	--	------------------------

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
			<p>insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V</a></p>	H-CIS-ASR_-050423/1326

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
			write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ASR_-050423/1327

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
<b>Product: asr_1002-x_r</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1328
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1329

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
			<p>to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1330

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
			condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: asr_1004</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1331
Improper Limitation of a Pathname	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	H-CIS-ASR_-050423/1332

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			<p>attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	ter/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1333

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
			<p>validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: asr_1006</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1334

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
			<p>commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-ASR_-050423/1335
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor</a></p>	H-CIS-ASR_-050423/1336

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
			<p>Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	y/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	

**Product: asr\_1006-x**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-xe-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-xe-</a></p>	H-CIS-ASR_-050423/1337
-----	-------------	-----	---	--	------------------------

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
			<p>CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	sdwan-VQAhejYw	
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1338

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
			<p>escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ASR_-050423/1339

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ASR_-050423/1340
<b>Product: asr_1009-x</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-ASR_-050423/1341

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
			<p>authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw</p>	
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a></p>	H-CIS-ASR_-050423/1342

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
			<p>affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-ASR_-050423/1343

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
			<p>UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1344

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
<b>Product: asr_1013</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1345
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1346

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
			<p>to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1347

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
			condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: asr_1023</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1348
Improper Limitation of a Pathname	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	H-CIS-ASR_-050423/1349

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			<p>attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	ter/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1350

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
			<p>validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: asr_900</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1351

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
			<p>commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-ASR_-050423/1352
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor</a></p>	H-CIS-ASR_-050423/1353

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
			<p>Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	y/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	

**Product: asr\_9000**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-iox-priv-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-iox-priv-</a></p>	H-CIS-ASR_-050423/1354
-----	-------------	-----	---	--	------------------------

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
			<p>insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V</a></p>	H-CIS-ASR_-050423/1355

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
			write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ASR_-050423/1356

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
<b>Product: asr_9000v</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1357
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1358

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
			<p>to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1359

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
			condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
Affected Version(s): v2					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1360
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a	<a href="https://sec.cloudapps.cisco.com/security/center/content">https://sec.cloudapps.cisco.com/security/center/content</a>	H-CIS-ASR_-050423/1361

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
Restricted Directory ('Path Traversal')			<p>directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthdi-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthdi-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1362

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
			<p>messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: asr_9001</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1363

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
			underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1364
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software,	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a>	H-CIS-ASR_-050423/1365

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
			<p>Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	asaftdios-dhcpv6-cli-Zf3zTv	
<b>Product: asr_9006</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-</a>	H-CIS-ASR_-050423/1366

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
			<p>on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ASR_-050423/1367

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
			<b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1368
<b>Product: asr_901-12c-f-d</b>					
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	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1369
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-ASR_-050423/1370

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
			<p>allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
<b>Product: asr_901-12c-ft-d</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1371

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1372
<b>Product: asr_901-4c-f-d</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-</a>	H-CIS-ASR_-050423/1373

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
			<p>on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ASR_-050423/1374

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
			<b>CVE ID : CVE-2023-20066</b>		
<b>Product: asr_901-4c-ft-d</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1375
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration.</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1376

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
			<p>An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		

**Product: asr\_901-6cz-f-a**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1377
-----	-------------	-----	---	--	------------------------

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
			system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-ASR_-050423/1378
<b>Product: asr_901-6cz-f-d</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a>	H-CIS-ASR_-050423/1379

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
			<p>attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	rityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-ASR_-050423/1380

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
<b>Product: asr_901-6cz-fs-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1381
Improper Limitation of a Pathname to a Restricted Directory	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor</a>	H-CIS-ASR_-050423/1382

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
('Path Traversal')			<p>outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	y/cisco-sa-webui-pthtrves7GSb9V	

**Product: asr\_901-6cz-fs-d**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1383
-----	-------------	-----	--	--	------------------------

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
			allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1384
<b>Product: asr_901-6cz-ft-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application	<a href="https://sec.cloudapps.c">https://sec.cloudapps.c</a>	H-CIS-ASR_-050423/1385

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
			<p>hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	<p>H-CIS-ASR_-050423/1386</p>

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
			are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>		
<b>Product: asr_901-6cz-ft-d</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.  <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1387
Improper Limitation of a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-ASR_-050423/1388

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			<p>authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p>security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</p>	
<b>Product: asr_9010</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR-050423/1389

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ASR_-050423/1390

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ASR_-050423/1391
<b>Product: asr_901s-2sg-f-ah</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-ASR_-050423/1392

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-ASR_-050423/1393</p>

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
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
<b>Product: asr_901s-2sg-f-d</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1394
Improper Limitation of a Pathname	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	H-CIS-ASR_-050423/1395

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			<p>attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	ter/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V	
<b>Product: asr_901s-3sg-f-ah</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1396

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
			<p>escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ASR_-050423/1397
<b>Product: asr_901s-3sg-f-d</b>					

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): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1398
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-ASR_-050423/1399

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
			<p>successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
<b>Product: asr_901s-4sg-f-d</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1400

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 Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1401
<b>Product: asr_902</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-</a>	H-CIS-ASR_-050423/1402

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
			<p>on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ASR_-050423/1403

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
			<b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1404
<b>Product: asr_902u</b>					
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	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1405
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-ASR_-050423/1406

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
			<p>allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1407

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
			vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: asr_903</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1408
Improper Limitation of a Pathname to a Restricted	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a>	H-CIS-ASR_-050423/1409

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			<p>access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	rityAdvisor y/cisco-sa- webui- pthtrv- es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ASR_-050423/1410

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: asr\_907**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1411
-----	-------------	-----	---	--	------------------------

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
			system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-ASR_-050423/1412
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-</a>	H-CIS-ASR_-050423/1413

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
			<p>Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	dhcpx6-cl- Zf3zTv	

**Product: asr\_914**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application.</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1414
-----	-------------	-----	--	---	------------------------

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
			<p>An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ASR_-050423/1415

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
			<b>CVE ID : CVE-2023-20066</b>		
<b>Product: asr_920-10sz-pd</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1416
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration.</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1417

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
			<p>An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
<b>Product: asr_920-10sz-pd_r</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1418

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
			system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-ASR_-050423/1419
<b>Product: asr_920-12cz-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a>	H-CIS-ASR_-050423/1420

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
			<p>attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	rityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-ASR_-050423/1421

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
			filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
<b>Product: asr_920-12cz-a_r</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1422
Improper Limitation of a Pathname to a Restricted Directory	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor</a>	H-CIS-ASR_-050423/1423

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
('Path Traversal')			<p>outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	y/cisco-sa-webui-pthtrves7GSb9V	

**Product: asr\_920-12cz-d**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1424
-----	-------------	-----	--	--	------------------------

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
			allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1425
<b>Product: asr_920-12cz-d_r</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application	<a href="https://sec.cloudapps.c">https://sec.cloudapps.c</a>	H-CIS-ASR_-050423/1426

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
			<p>hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that</p>	<p>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V</p>	<p>H-CIS-ASR_-050423/1427</p>

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
			are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>		
<b>Product: asr_920-12sz-im</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.  <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1428
Improper Limitation of a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-ASR_-050423/1429

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			<p>authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p>security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</p>	
<b>Product: asr_920-12sz-im_r</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR-050423/1430

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ASR_-050423/1431

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
<b>Product: asr_920-24sz-im</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1432
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1433

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
			<p>to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
<b>Product: asr_920-24sz-im_r</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1434

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-ASR_-050423/1435
<b>Product: asr_920-24sz-m</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a>	H-CIS-ASR_-050423/1436

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
			<p>affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-ASR_-050423/1437

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
			UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
<b>Product: asr_920-24sz-m_r</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1438
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-ASR_-050423/1439

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
<b>Product: asr_920-24tz-m</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1440

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
			commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-ASR_-050423/1441
<b>Product: asr_920-24tz-m_r</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	H-CIS-ASR_-050423/1442

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
			<p>could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	<p>H-CIS-ASR_-050423/1443</p>

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
			<p>UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
<b>Product: asr_920-4sz-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1444
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content">https://sec.cloudapps.cisco.com/security/center/content</a></p>	H-CIS-ASR_-050423/1445

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
Restricted Directory ('Path Traversal')			<p>directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V	
<b>Product: asr_920-4sz-a_r</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1446

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
			<p>application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-ASR_-050423/1447
<b>Product: asr_920-4sz-d</b>					
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	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1448
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-ASR_-050423/1449

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
			<p>allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
<b>Product: asr_920-4sz-d_r</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1450

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 Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1451
<b>Product: asr_920u-12sz-im</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-</a>	H-CIS-ASR_-050423/1452

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
			<p>on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ASR_-050423/1453

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
			<b>CVE ID : CVE-2023-20066</b>		
<b>Product: asr_9901</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1454
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration.</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1455

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
			<p>An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		

**Product: asr\_9902**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1456
-----	-------------	-----	---	--	------------------------

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
			system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-ASR_-050423/1457
<b>Product: asr_9903</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a>	H-CIS-ASR_-050423/1458

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
			<p>attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	rityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-ASR_-050423/1459

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
			<p>filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
<b>Product: asr_9904</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1460
Improper Limitation of a Pathname to a Restricted Directory	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor</a></p>	H-CIS-ASR_-050423/1461

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
('Path Traversal')			<p>outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	y/cisco-sa-webui-pthtrves7GSb9V	

**Product: asr\_9906**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1462
-----	-------------	-----	--	--	------------------------

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
			allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1463
<b>Product: asr_9910</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application	<a href="https://sec.cloudapps.c">https://sec.cloudapps.c</a>	H-CIS-ASR_-050423/1464

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
			<p>hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	<p>H-CIS-ASR_-050423/1465</p>

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
			are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>		
<b>Product: asr_9912</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.  <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1466
Improper Limitation of a	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-ASR_-050423/1467

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			<p>authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p>security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</p>	
<b>Product: asr_9920</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ASR_-050423/1468

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ASR_-050423/1469

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
<b>Product: asr_9922</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ASR_-050423/1470
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ASR_-050423/1471

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
			<p>to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		

**Product: catalyst\_3650**

Affected Version(s): -

Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafdi-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafdi-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1472
---------------------	-------------	-----	---	--	------------------------

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
			<p>device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_3650-12x48fd-e</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1473

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
			successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3650-12x48fd-1</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1474

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
			<p>either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_3650-12x48fd-s</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1475

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
			man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3650-12x48uq</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1476

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
			<b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3650-12x48uq-e</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1477

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
<b>Product: catalyst_3650-12x48uq-l</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1478
<b>Product: catalyst_3650-12x48uq-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1479
<b>Product: catalyst_3650-12x48ur</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1480
<b>Product: catalyst_3650-12x48ur-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1481
<b>Product: catalyst_3650-12x48ur-1</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1482
<b>Product: catalyst_3650-12x48ur-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1483
<b>Product: catalyst_3650-12x48uz</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1484
<b>Product: catalyst_3650-12x48uz-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1485
<b>Product: catalyst_3650-12x48uz-l</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1486
<b>Product: catalyst_3650-12x48uz-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1487
<b>Product: catalyst_3650-24pd</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1488
<b>Product: catalyst_3650-24pd-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1489
<b>Product: catalyst_3650-24pd-1</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1490
<b>Product: catalyst_3650-24pd-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1491
<b>Product: catalyst_3650-24pdm</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1492
<b>Product: catalyst_3650-24pdm-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1493
<b>Product: catalyst_3650-24pdm-l</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1494
<b>Product: catalyst_3650-24pdm-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1495
<b>Product: catalyst_3650-24ps-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1496
<b>Product: catalyst_3650-24ps-l</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1497
<b>Product: catalyst_3650-24ps-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1498
<b>Product: catalyst_3650-24td-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1499
<b>Product: catalyst_3650-24td-l</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1500
<b>Product: catalyst_3650-24td-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1501
<b>Product: catalyst_3650-24ts-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1502
<b>Product: catalyst_3650-24ts-l</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1503
<b>Product: catalyst_3650-24ts-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1504
<b>Product: catalyst_3650-48fd-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1505
<b>Product: catalyst_3650-48fd-l</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1506
<b>Product: catalyst_3650-48fd-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1507
<b>Product: catalyst_3650-48fq</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1508
<b>Product: catalyst_3650-48fq-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1509
<b>Product: catalyst_3650-48fq-l</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1510
<b>Product: catalyst_3650-48fq-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1511
<b>Product: catalyst_3650-48fqm</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1512
<b>Product: catalyst_3650-48fqm-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1513
<b>Product: catalyst_3650-48fqm-l</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1514
<b>Product: catalyst_3650-48fqm-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1515
<b>Product: catalyst_3650-48fs-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1516
<b>Product: catalyst_3650-48fs-l</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1517
<b>Product: catalyst_3650-48fs-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1518
<b>Product: catalyst_3650-48pd-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1519
<b>Product: catalyst_3650-48pd-1</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1520
<b>Product: catalyst_3650-48pd-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1521
<b>Product: catalyst_3650-48pq-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1522
<b>Product: catalyst_3650-48pq-l</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1523
<b>Product: catalyst_3650-48pq-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1524
<b>Product: catalyst_3650-48ps-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1525
<b>Product: catalyst_3650-48ps-l</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1526
<b>Product: catalyst_3650-48ps-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1527
<b>Product: catalyst_3650-48td-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1528
<b>Product: catalyst_3650-48td-l</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1529
<b>Product: catalyst_3650-48td-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1530
<b>Product: catalyst_3650-48tq-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1531
<b>Product: catalyst_3650-48tq-l</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1532
<b>Product: catalyst_3650-48tq-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1533
<b>Product: catalyst_3650-48ts-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1534
<b>Product: catalyst_3650-48ts-l</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1535
<b>Product: catalyst_3650-48ts-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1536
<b>Product: catalyst_3650-8x24pd-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1537
<b>Product: catalyst_3650-8x24pd-1</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1538
<b>Product: catalyst_3650-8x24pd-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1539
<b>Product: catalyst_3650-8x24uq</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1540
<b>Product: catalyst_3650-8x24uq-e</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1541
<b>Product: catalyst_3650-8x24uq-l</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1542
<b>Product: catalyst_3650-8x24uq-s</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1543
<b>Product: catalyst_3850</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1544

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1545</p>

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
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1546

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3850-12s-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1547
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1548

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1549

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_3850-12s-s**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1550
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1551
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1552

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_3850-12x48u</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1553

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1554

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1555
<b>Product: catalyst_3850-12xs-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1556

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1557</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1558

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3850-12xs-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1559
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1560

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1561

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_3850-16xs-e**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1562
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1563
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1564

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_3850-16xs-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1565

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1566

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1567
<b>Product: catalyst_3850-24p-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1568

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1569</p>

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
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1570

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3850-24p-1</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1571
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1572

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1573

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_3850-24p-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1574

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1575
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1576

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_3850-24pw-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1577

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1578

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1579
<b>Product: catalyst_3850-24s-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1580

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1581</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafthd-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafthd-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1582

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3850-24s-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1583
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1584

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1585

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_3850-24t-e**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1586
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1587
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1588

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_3850-24t-1</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1589

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1590

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1591
<b>Product: catalyst_3850-24t-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1592

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1593</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1594

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3850-24u</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1595
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1596

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1597

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_3850-24u-e**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1598
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1599
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1600

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_3850-24u-l</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1601

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1602

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1603
<b>Product: catalyst_3850-24u-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1604

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1605</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1606

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3850-24xs</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1607
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1608

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1609

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_3850-24xs-e**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1610
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1611
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1612

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_3850-24xs-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1613

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1614

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1615
<b>Product: catalyst_3850-24xu</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1616

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1617</p>

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
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1618

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3850-24xu-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1619
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1620

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1621

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_3850-24xu-1**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1622
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1623
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1624

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_3850-24xu-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1625

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1626

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1627
<b>Product: catalyst_3850-32xs-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1628

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1629</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1630

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3850-32xs-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1631
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1632

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1633

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_3850-48f-e**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1634
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1635
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1636

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_3850-48f-1</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1637

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1638

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1639
<b>Product: catalyst_3850-48f-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1640

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1641</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1642

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3850-48p-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1643
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1644

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1645

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_3850-48p-1**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1646
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1647
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1648

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_3850-48p-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1649

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	<p>H-CIS-CATA-050423/1650</p>

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1651
<b>Product: catalyst_3850-48pw-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1652

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1653</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1654

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3850-48t-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1655
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1656

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1657

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_3850-48t-1**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1658
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1659
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1660

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_3850-48t-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1661

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1662

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1663
<b>Product: catalyst_3850-48u</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1664

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1665</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1666

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3850-48u-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1667
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1668

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1669

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_3850-48u-1**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1670
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1671
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1672

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_3850-48u-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1673

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1674

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1675
<b>Product: catalyst_3850-48xs</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1676

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1677</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1678

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3850-48xs-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1679
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1680

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1681

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_3850-48xs-f-e**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1682
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1683
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1684

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_3850-48xs-f-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1685

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1686

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1687
<b>Product: catalyst_3850-48xs-s</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1688

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1689</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1690

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_3850-nm-2-40g</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1691
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1692

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1693

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_3850-nm-8-10g**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1694
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1695
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1696

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_8200</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw</a></p>	H-CIS-CATA-050423/1697

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
			<p>authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>		
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1698

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
			execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1699
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a>	H-CIS-CATA-050423/1700

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
			<p>Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://securityadvisors.cisco.com/advisory/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">rityAdvisor y/cisco-sa- asaftdios- dhcpv6-cli- Zf3zTv</a>	
<b>Product: catalyst_8300</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input</p>	<a href="https://securityadvisors.cisco.com/securitycenter/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-">https://sec. cloudapps.c isco.com/s ecurity/cen ter/content /CiscoSecu rityAdvisor y/cisco-sa- ios-xe-</a>	H-CIS-CATA-050423/1701

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
			<p>validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	sdwan-VQAhejYw	
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1702

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1703

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
<b>Product: catalyst_8300-1n1s-4t2x</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw</a></p>	H-CIS-CATA-050423/1704
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<p><a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a></p>	H-CIS-CATA-050423/1705

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1706</p>

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
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1707

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_8300-1n1s-6t</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts,	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw</a>	H-CIS-CATA-050423/1708

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
			see the Details section of this advisory. <b>CVE ID : CVE-2023-20035</b>		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1709
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1710

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
			<p>this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1711

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
			<p>device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_8300-2n2s-4t2x</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhejYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhejYw</a></p>	H-CIS-CATA-050423/1712

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
			vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. <b>CVE ID : CVE-2023-20035</b>		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1713
Improper Limitation of a Pathname to a Restricted Directory	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a>	H-CIS-CATA-050423/1714

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
('Path Traversal')			<p>mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	webui-pthtrves7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1715

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
			<p>crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_8300-2n2s-6t**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw</a></p>	H-CIS-CATA-050423/1716
-----	-------------	-----	--	--	------------------------

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
			<p>the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>		
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1717
Improper Limitation of a	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a></p>	H-CIS-CATA-050423/1718

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			<p>authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p>security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</p>	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1719

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
			<p>is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_8500**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhejYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhejYw</a></p>	H-CIS-CATA-050423/1720
-----	-------------	-----	---	--	------------------------

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
			<p>submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>		
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1721

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V</a>	H-CIS-CATA-050423/1722
<b>Product: catalyst_8500-4qc</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a>	H-CIS-CATA-050423/1723

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
			<p>insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	ios-xe-sdwan-VQAhEjYw	
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1724

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
			<p>this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1725

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1726
<b>Product: catalyst_8500l</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1727

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
			<p>authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhejYw</p>	
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a></p>	H-CIS-CATA-050423/1728

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
			<p>affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1729

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
			<p>UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1730

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
<b>Product: catalyst_8510csr</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw</a></p>	H-CIS-CATA-050423/1731
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<p><a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a></p>	H-CIS-CATA-050423/1732

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1733</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1734

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_8510msr</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts,	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw</a>	H-CIS-CATA-050423/1735

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
			see the Details section of this advisory. <b>CVE ID : CVE-2023-20035</b>		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1736
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-CATA-050423/1737

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
			<p>this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1738

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
			<p>device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_8540csr</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAHEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAHEjYw</a></p>	H-CIS-CATA-050423/1739

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
			vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory. <b>CVE ID : CVE-2023-20035</b>		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1740
Improper Limitation of a Pathname to a Restricted Directory	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a>	H-CIS-CATA-050423/1741

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
('Path Traversal')			<p>mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	webui-pthtrves7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1742

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
			<p>crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_8540msr**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAHEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAHEjYw</a></p>	H-CIS-CATA-050423/1743
-----	-------------	-----	--	--	------------------------

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
			<p>the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>		
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1744
Improper Limitation of a	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a></p>	H-CIS-CATA-050423/1745

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			<p>authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p>security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</p>	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1746

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
			<p>is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_9100**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-CATA-050423/1747
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: catalyst\_9105**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1748
-----	-------------	-----	---	---	------------------------

**Product: catalyst\_9105ax**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1749
-----	-------------	-----	--	---	------------------------

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: catalyst\_9105axi**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-CATA-050423/1750
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: catalyst\_9105axw**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1751
-----	-------------	-----	---	---	------------------------

**Product: catalyst\_9115**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1752
-----	-------------	-----	--	---	------------------------

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: catalyst\_9115ax**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-CATA-050423/1753
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: catalyst\_9115axe**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1754
-----	-------------	-----	---	---	------------------------

**Product: catalyst\_9115axi**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	H-CIS-CATA-050423/1755
-----	-------------	-----	--	---	------------------------

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: catalyst\_9115\_ap**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-CATA-050423/1756
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: catalyst\_9117**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1757
-----	-------------	-----	---	---	------------------------

**Product: catalyst\_9117ax**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	H-CIS-CATA-050423/1758
-----	-------------	-----	--	---	------------------------

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: catalyst\_9117axi**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-CATA-050423/1759
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: catalyst\_9117\_ap**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1760
-----	-------------	-----	---	---	------------------------

**Product: catalyst\_9120**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1761
-----	-------------	-----	--	---	------------------------

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: catalyst\_9120ax**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-CATA-050423/1762
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: catalyst\_9120axe**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1763
-----	-------------	-----	---	---	------------------------

**Product: catalyst\_9120axi**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1764
-----	-------------	-----	--	---	------------------------

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: catalyst\_9120axp**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-CATA-050423/1765
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: catalyst\_9120\_ap**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1766
-----	-------------	-----	---	---	------------------------

**Product: catalyst\_9124**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1767
-----	-------------	-----	--	---	------------------------

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: catalyst\_9124ax**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-CATA-050423/1768
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: catalyst\_9124axd**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1769
-----	-------------	-----	---	---	------------------------

**Product: catalyst\_9124axi**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1770
-----	-------------	-----	--	---	------------------------

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: catalyst\_9130**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-CATA-050423/1771
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: catalyst\_9130ax**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1772
-----	-------------	-----	---	---	------------------------

**Product: catalyst\_9130axe**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1773
-----	-------------	-----	--	---	------------------------

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
			<p>authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</p>	

**Product: catalyst\_9130axi**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-CATA-050423/1774
-----	-------------	-----	--	--	------------------------

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
			exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		

**Product: catalyst\_9130\_ap**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1775
-----	-------------	-----	---	---	------------------------

**Product: catalyst\_9200**

Affected Version(s): -

N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-app-hosting-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-app-hosting-dos-tc2EKEpu</a>	H-CIS-CATA-050423/1776
-----	-------------	-----	---	---	------------------------

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
			<p>could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	<p>H-CIS-CATA-050423/1777</p>

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
			<p>UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1778

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
			man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9200cx</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1779
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-</a>	H-CIS-CATA-050423/1780

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
			<p>due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1781

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
			<p>device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9200l</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1782

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1783
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1784

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9300</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1785

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note:</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1786

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
			<p>In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1787

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
			<b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1788
<b>Product: catalyst_9300-24p-a</b>					
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	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1789
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spiface-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spiface-yejYgnNQ</a>	H-CIS-CATA-050423/1790

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
			<p>for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1791

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
			<p>to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1792

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
			condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9300-24p-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1793
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	H-CIS-CATA-050423/1794

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
			<p>authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>	<a href="https://content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ">ter/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ</a>	
Improper Limitation	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE	<a href="https://sec.cloudapps.c">https://sec.cloudapps.c</a>	H-CIS-CATA-050423/1795

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
of a Pathname to a Restricted Directory ('Path Traversal')			<p>Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<a href="https://www.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a>	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected</p>	<a href="https://www.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dhcpv6-cli-Zf3zTv">https://www.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1796

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
			<p>device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_9300-24s-a**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1797
-----	-------------	-----	--	--	------------------------

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
			allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a>	H-CIS-CATA-050423/1798

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
			<p>vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-CATA-050423/1799

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1800
<b>Product: catalyst_9300-24s-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1801

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1802

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
			<p>vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1803

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
			<p>read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1804

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9300-24t-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1805
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor</a>	H-CIS-CATA-050423/1806

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
			<p>unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>	y/cisco-sa-c9300-spi-ace-yejYgnNQ	
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a</p>	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-CATA-050423/1807

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
Restricted Directory ('Path Traversal')			<p>directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthdi-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthdi-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1808

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
			<p>messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_9300-24t-e**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1809
-----	-------------	-----	--	--	------------------------

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
			underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a>	H-CIS-CATA-050423/1810

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
			could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. <b>CVE ID : CVE-2023-20082</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1811
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a>	H-CIS-CATA-050423/1812

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
			<p>Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://securityadvisory.cisco.com/sasaftdios-dhcpv6-cli-Zf3zTv">rityAdvisor y/cisco-sa-saftdios-dhcpv6-cli-Zf3zTv</a>	
<b>Product: catalyst_9300-24u-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This</p>	<a href="https://securityadvisory.cisco.com/security/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-">https://securityadvisory.cisco.com/security/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-</a>	H-CIS-CATA-050423/1813

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
			<p>vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	escalate-Xg8zkyPk	
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1814

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
			<p>successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-CATA-050423/1815

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
			<p>maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1816

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
			<b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9300-24u-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1817
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a>	H-CIS-CATA-050423/1818

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
			<p>of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a></p>	H-CIS-CATA-050423/1819

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
			<p>due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafdi-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafdi-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1820

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
			<p>device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9300-24ux-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1821

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
			<b>CVE ID : CVE-2023-20065</b>		
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1822

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
			that would lower the attack complexity. <b>CVE ID : CVE-2023-20082</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-CATA-050423/1823
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-</a>	H-CIS-CATA-050423/1824

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
			<p>Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	dhcpx6-cl-Zf3zTv	

**Product: catalyst\_9300-24ux-e**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1825
-----	-------------	-----	--	--	------------------------

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
			<p>An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1826

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
			<p>on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtraves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtraves7GSb9V</a></p>	H-CIS-CATA-050423/1827

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
			write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1828

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
<b>Product: catalyst_9300-48p-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1829
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a>	H-CIS-CATA-050423/1830

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
			<p>retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-CATA-050423/1831

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
			<p>this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1832

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
			device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9300-48p-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1833
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco	<a href="https://sec.cloudapps.c">https://sec.cloudapps.c</a>	H-CIS-CATA-050423/1834

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
			<p>Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>	<p>isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ</p>	

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 Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1835
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1836

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
			<p>of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9300-48s-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1837

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
			<p>application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1838

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
			<p>later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1839

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1840
<b>Product: catalyst_9300-48s-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1841

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1842

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
			<p>vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1843

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
			<p>read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1844

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9300-48t-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1845
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor</a>	H-CIS-CATA-050423/1846

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
			<p>unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>	y/cisco-sa-c9300-spi-ace-yejYgnNQ	
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content">https://sec.cloudapps.cisco.com/security/center/content</a>	H-CIS-CATA-050423/1847

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
Restricted Directory ('Path Traversal')			<p>directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthdi-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthdi-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1848

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
			<p>messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9300-48t-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1849

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
			underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-aceyjYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-aceyjYgnNQ</a>	H-CIS-CATA-050423/1850

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
			could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. <b>CVE ID : CVE-2023-20082</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1851
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a>	H-CIS-CATA-050423/1852

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
			<p>Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	rityAdvisor y/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv	
<b>Product: catalyst_9300-48u-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-</a>	H-CIS-CATA-050423/1853

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
			<p>vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	escalate-Xg8zkyPk	
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1854

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
			<p>successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1855

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
			maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1856

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
			<b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9300-48u-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1857
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1858

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
			<p>of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a></p>	H-CIS-CATA-050423/1859

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
			<p>due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1860

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
			<p>device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9300-48un-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1861

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
			<b>CVE ID : CVE-2023-20065</b>		
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1862

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
			that would lower the attack complexity. <b>CVE ID : CVE-2023-20082</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-CATA-050423/1863
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-</a>	H-CIS-CATA-050423/1864

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
			<p>Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	dhcpx6-cl- Zf3zTv	

**Product: catalyst\_9300-48un-e**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application.</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1865
-----	-------------	-----	--	---	------------------------

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
			<p>An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1866

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
			<p>on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtraves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtraves7GSb9V</a></p>	H-CIS-CATA-050423/1867

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
			write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1868

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
<b>Product: catalyst_9300-48uxm-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1869
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a>	H-CIS-CATA-050423/1870

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
			<p>retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-CATA-050423/1871

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
			<p>this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1872

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
			device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9300-48uxm-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1873
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco	<a href="https://sec.cloudapps.c">https://sec.cloudapps.c</a>	H-CIS-CATA-050423/1874

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
			<p>Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>	<p>isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ</p>	

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 Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1875
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1876

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
			<p>of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9300l</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1877

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
			<p>application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spiface-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spiface-yejYgnNQ</a></p>	H-CIS-CATA-050423/1878

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
			<p>later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1879

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1880
<b>Product: catalyst_9300l-24p-4g-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1881

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1882

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
			<p>vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-CATA-050423/1883

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
			<p>read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1884

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9300l-24p-4g-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1885
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor</a>	H-CIS-CATA-050423/1886

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
			<p>unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>	y/cisco-sa-c9300-spi-ace-yejYgnNQ	
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a</p>	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-CATA-050423/1887

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
Restricted Directory ('Path Traversal')			<p>directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthd-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthd-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1888

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
			<p>messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9300l-24p-4x-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1889

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
			underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-aceyYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-aceyYgnNQ</a>	H-CIS-CATA-050423/1890

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
			could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. <b>CVE ID : CVE-2023-20082</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1891
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a>	H-CIS-CATA-050423/1892

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
			<p>Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://securityadvisory.cisco.com/sasaftdios-dhcpv6-cli-Zf3zTv">rityAdvisor y/cisco-sa-sasaftdios-dhcpv6-cli-Zf3zTv</a>	
<b>Product: catalyst_9300l-24p-4x-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This</p>	<a href="https://securityadvisory.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-</a>	H-CIS-CATA-050423/1893

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
			<p>vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	escalate-Xg8zkyPk	
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1894

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
			<p>successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-CATA-050423/1895

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
			<p>maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1896

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
			<b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9300l-24t-4g-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1897
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a>	H-CIS-CATA-050423/1898

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
			<p>of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a></p>	H-CIS-CATA-050423/1899

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
			<p>due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafdi-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafdi-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1900

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
			<p>device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9300l-24t-4g-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1901

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
			<b>CVE ID : CVE-2023-20065</b>		
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1902

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
			that would lower the attack complexity. <b>CVE ID : CVE-2023-20082</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-CATA-050423/1903
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-</a>	H-CIS-CATA-050423/1904

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
			<p>Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	dhcpx6-cl- Zf3zTv	

**Product: catalyst\_9300l-24t-4x-a**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application.</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1905
-----	-------------	-----	--	---	------------------------

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
			<p>An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1906

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
			<p>on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1907

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
			write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1908

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
<b>Product: catalyst_9300l-24t-4x-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1909
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a>	H-CIS-CATA-050423/1910

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
			<p>retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-CATA-050423/1911

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
			<p>this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1912

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
			device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9300l-48p-4g-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1913
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco	<a href="https://sec.cloudapps.c">https://sec.cloudapps.c</a>	H-CIS-CATA-050423/1914

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
			<p>Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>	<p>isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ</p>	

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 Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1915
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1916

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
			<p>of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9300l-48p-4g-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1917

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
			<p>application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spiface-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spiface-yejYgnNQ</a></p>	H-CIS-CATA-050423/1918

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
			<p>later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1919

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1920
<b>Product: catalyst_9300l-48p-4x-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1921

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1922

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
			<p>vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1923

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
			<p>read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1924

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9300l-48p-4x-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1925
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor</a>	H-CIS-CATA-050423/1926

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
			<p>unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>	y/cisco-sa-c9300-spi-ace-yejYgnNQ	
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a</p>	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-CATA-050423/1927

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
Restricted Directory ('Path Traversal')			<p>directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthd-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthd-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1928

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
			<p>messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9300l-48t-4g-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1929

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
			underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a>	H-CIS-CATA-050423/1930

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
			could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. <b>CVE ID : CVE-2023-20082</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1931
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a>	H-CIS-CATA-050423/1932

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
			<p>Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://securityadvisory.cisco.com/sasaftdios-dhcpv6-cli-Zf3zTv">rityAdvisor y/cisco-sa-saftdios-dhcpv6-cli-Zf3zTv</a>	
<b>Product: catalyst_9300l-48t-4g-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This</p>	<a href="https://securityadvisory.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-">https://securityadvisory.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-</a>	H-CIS-CATA-050423/1933

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
			<p>vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	escalate-Xg8zkyPk	
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1934

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
			<p>successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1935

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
			maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1936

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
			<b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9300l-48t-4x-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1937
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a>	H-CIS-CATA-050423/1938

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
			<p>of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a></p>	H-CIS-CATA-050423/1939

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
			<p>due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafdi-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafdi-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1940

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
			<p>device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9300l-48t-4x-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1941

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
			<b>CVE ID : CVE-2023-20065</b>		
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1942

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
			that would lower the attack complexity. <b>CVE ID : CVE-2023-20082</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-CATA-050423/1943
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-</a>	H-CIS-CATA-050423/1944

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
			<p>Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	dhcpx6-cl-Zf3zTv	

**Product: catalyst\_9300lm**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1945
-----	-------------	-----	--	--	------------------------

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
			<p>An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	H-CIS-CATA-050423/1946

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
			<p>on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1947

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
			write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1948

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
<b>Product: catalyst_9300l_stack</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1949
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a>	H-CIS-CATA-050423/1950

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
			<p>retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-CATA-050423/1951

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
			<p>this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1952

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
			device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9300x</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1953
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco	<a href="https://sec.cloudapps.c">https://sec.cloudapps.c</a>	H-CIS-CATA-050423/1954

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
			<p>Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>	<p>isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ</p>	

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 Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1955
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1956

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
			<p>of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9400</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1957

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
			<p>application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-CATA-050423/1958

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1959
<b>Product: catalyst_9400_supervisor_engine-1</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1960

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1961</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1962

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9407r</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1963
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1964

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1965

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_9410r**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1966
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1967
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1968

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9500</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1969

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1970

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1971
<b>Product: catalyst_9500h</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1972

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1973</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1974

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9600</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1975
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1976

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1977

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_9600x**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1978
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1979
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1980

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9600_supervisor_engine-1</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1981

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1982

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1983
<b>Product: catalyst_9800</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1984

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1985</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1986

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9800-40</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1987
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/1988

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1989

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_9800-40\_wireless\_controller**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1990
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/1991
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1992

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9800-80</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/1993

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/1994

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/1995
<b>Product: catalyst_9800-80_wireless_controller</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/1996

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/1997</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/1998

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9800-cl</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/1999
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/2000

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/2001

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_9800-1**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/2002
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CATA-050423/2003
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/2004

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: catalyst_9800-l-c</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/2005

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-CATA-050423/2006

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/2007
<b>Product: catalyst_9800-l-f</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-CATA-050423/2008

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-CATA-050423/2009</p>

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
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-CATA-050423/2010

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: catalyst_9800_embedded_wireless_controller</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/2011
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/2012

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CATA-050423/2013

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: catalyst\_ie3200**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/2014
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-phtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-phtrves7GSb9V</a>	H-CIS-CATA-050423/2015
<b>Product: catalyst_ie3200_rugged_switch</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a>	H-CIS-CATA-050423/2016

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
			<p>affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-CATA-050423/2017

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
			UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
<b>Product: catalyst_ie3300</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-CATA-050423/2018
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-CATA-050423/2019

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	

**Product: catalyst\_ie3300\_rugged\_switch**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/2020
-----	-------------	-----	--	--	------------------------

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
			commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-CATA-050423/2021
<b>Product: catalyst_ie3400</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	H-CIS-CATA-050423/2022

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
			could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	ter/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-CATA-050423/2023

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
			<p>UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
<b>Product: catalyst_ie3400_heavy_duty_switch</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/2024
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content">https://sec.cloudapps.cisco.com/security/center/content</a></p>	H-CIS-CATA-050423/2025

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
Restricted Directory ('Path Traversal')			<p>directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V	
<b>Product: catalyst_ie3400_rugged_switch</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/2026

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
			<p>application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-CATA-050423/2027
<b>Product: catalyst_ie9300</b>					
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	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CATA-050423/2028
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-CATA-050423/2029

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
			<p>allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		

**Product: catalyst\_iw6300**

Affected Version(s): -

N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	H-CIS-CATA-050423/2030
-----	-------------	-----	--	--	------------------------

**Product: catalyst\_iw6300\_ac**

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): -					
N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/2031

**Product: catalyst\_iw6300\_dc**

Affected Version(s): -					
N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/2032

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
			could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.  <b>CVE ID : CVE-2023-20056</b>		

**Product: catalyst\_iw6300\_dcw**

Affected Version(s): -

N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.  <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-CATA-050423/2033
-----	-------------	-----	---	---	------------------------

**Product: cbr-8**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CBR--050423/2034
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-CBR--050423/2035

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
			<p>successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		

**Product: cbr8\_converged\_broadband\_router**

Affected Version(s): -

Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload,</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CBR8-050423/2036
---------------------	-------------	-----	---	--	------------------------

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
			<p>resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: cg418-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CG41-050423/2037
Improper Limitation of a	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a></p>	H-CIS-CG41-050423/2038

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			<p>authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p>security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</p>	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-CG41-050423/2039

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
			<p>is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: cg522-e**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-CG52-050423/2040
-----	-------------	-----	--	--	------------------------

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
			execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-CG52-050423/2041
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a>	H-CIS-CG52-050423/2042

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
			<p>Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	rityAdvisor/cisco-sa-saftdios-dhcpv6-cli-Zf3zTv	
<b>Product: cloud_services_router_1000v</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-saftdios-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-saftdios-</a></p>	H-CIS-CLOU-050423/2043

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
			<p>Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	dhcpx6-cl-Zf3zTv	

**Product: csr\_1000v**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw</a>	H-CIS-CSR_-050423/2044
-----	-------------	-----	---	---	------------------------

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
			<p>commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>		
<b>Product: esr-6300-con-k9</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ESR--050423/2045

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
			<p>device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: esr-6300-ncp-k9**

Affected Version(s): -

Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ESR--050423/2046
---------------------	-------------	-----	---	--	------------------------

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
			<p>messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: esr6300</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ESR6-050423/2047

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
			underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ESR6-050423/2048
<b>Product: ess-3300-24t-con-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content">https://sec.cloudapps.cisco.com/security/center/content</a>	H-CIS-ESS--050423/2049

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
			<p>authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-ESS--050423/2050

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
			located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ESS--050423/2051

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
			man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: ess-3300-24t-con-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ESS--050423/2052
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-</a>	H-CIS-ESS--050423/2053

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
			<p>due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafdi-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafdi-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ESS--050423/2054

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
			<p>device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: ess-3300-24t-ncp-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ESS--050423/2055

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ESS--050423/2056
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ESS--050423/2057

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: ess-3300-24t-ncp-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ESS--050423/2058

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ESS--050423/2059

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ESS--050423/2060
<b>Product: ess-3300-con-a</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-ESS--050423/2061

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-ESS--050423/2062</p>

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
			mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ESS--050423/2063

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: ess-3300-con-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ESS--050423/2064
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-ESS--050423/2065

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ESS--050423/2066

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: ess-3300-ncp-a**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ESS--050423/2067
-----	-------------	-----	--	--	------------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ESS--050423/2068
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ESS--050423/2069

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: ess-3300-ncp-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ESS--050423/2070

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ESS--050423/2071

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ESS--050423/2072
<b>Product: ess9300-10x-e</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-ESS9-050423/2073

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-ESS9-050423/2074</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ESS9-050423/2075

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: esw6300</b>					
Affected Version(s): -					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	H-CIS-ESW6-050423/2076
<b>Product: ie-3200-8p2s-e</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a>	H-CIS-IE-3-050423/2077

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
			<p>Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://securityadvisors.cisco.com/advisory/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">rityAdvisor y/cisco-sa- asaftdios- dhcpv6-cli- Zf3zTv</a>	
<b>Product: ie-3200-8t2s-e</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and</p>	<a href="https://securityadvisors.cisco.com/advisory/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec. cloudapps.c isco.com/s ecurity/cen ter/content /CiscoSecu rityAdvisor y/cisco-sa- asaftdios-</a>	H-CIS-IE-3-050423/2078

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
			<p>Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	dhcpx6-cl-Zf3zTv	

**Product: ie-3300-8p2s-a**

Affected Version(s): -

Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cl-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cl-Zf3zTv</a></p>	H-CIS-IE-3-050423/2079
---------------------	-------------	-----	---	--	------------------------

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
			<p>attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: ie-3300-8p2s-e</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-IE-3-050423/2080

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
			<p>device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: ie-3300-8t2s-a**

Affected Version(s): -

Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-IE-3-050423/2081
---------------------	-------------	-----	---	--	------------------------

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
			<p>messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: ie-3300-8t2s-e</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafthd-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafthd-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-IE-3-050423/2082

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
			<p>crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: ie-3300-8t2x-a**

Affected Version(s): -

Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-IE-3-050423/2083
---------------------	-------------	-----	---	--	------------------------

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
			<p>exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: ie-3300-8t2x-e</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload,</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-IE-3-050423/2084

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
			<p>resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: ie-3300-8u2x-a</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-IE-3-050423/2085

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
			vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: ie-3300-8u2x-e</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafdi-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asafdi-dhcpv6-cli-Zf3zTv</a>	H-CIS-IE-3-050423/2086

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: ie-3400-8p2s-a</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-IE-3-050423/2087

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
			man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: ie-3400-8p2s-e</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-IE-3-050423/2088

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
			<b>CVE ID : CVE-2023-20081</b>		
<b>Product: ie-3400-8t2s-a</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-IE-3-050423/2089

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
<b>Product: ie-3400-8t2s-e</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-IE-3-050423/2090
<b>Product: ie-9310-26s2c</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-IE-9-050423/2091
<b>Product: ie-9320-26s2c</b>					
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
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-IE-9-050423/2092
<b>Product: integrated_services_virtual_router</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-INTE-050423/2093

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-INTE-050423/2094</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-INTE-050423/2095

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: isr_1000</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ISR_-050423/2096
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-ISR_-050423/2097

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	

**Product: isr\_1100**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw</a></p>	H-CIS-ISR_050423/2098
-----	-------------	-----	--	--	-----------------------

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
			<p>to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>		
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ISR_-050423/2099

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pathtrv-es7GSb9V</a>	H-CIS-ISR_050423/2100
<b>Product: isr_1100-4g</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a>	H-CIS-ISR_050423/2101

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
			<p>affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-ISR_050423/2102

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
			<p>UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ISR_050423/2103

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
<b>Product: isr_1100-4g\6g</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAHEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAHEjYw</a></p>	H-CIS-ISR_-050423/2104
<b>Product: isr_1100-4p</b>					
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	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw</a></p>	H-CIS-ISR_-050423/2105
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content">https://sec.cloudapps.cisco.com/security/center/content</a></p>	H-CIS-ISR_-050423/2106

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
			<p>authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-ISR_-050423/2107

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
			located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ISR_050423/2108

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
			man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: isr_1100-6g</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ISR_-050423/2109
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-</a>	H-CIS-ISR_-050423/2110

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
			<p>due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ISR_050423/2111

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
			<p>device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: isr_1100-8p</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw</a></p>	H-CIS-ISR_-050423/2112

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
			<p>privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>		
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ISR_050423/2113
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content">https://sec.cloudapps.cisco.com/security/center/content</a></p>	H-CIS-ISR_050423/2114

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
Restricted Directory ('Path Traversal')			<p>directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthdi-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthdi-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ISR_-050423/2115

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
			<p>messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: isr_1101</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw</a></p>	H-CIS-ISR_-050423/2116

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
			<p>successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>		
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ISR_-050423/2117

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 Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ISR_-050423/2118
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ISR_-050423/2119

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
			<p>of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: isr_1101-4p</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhejYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhejYw</a></p>	H-CIS-ISR_-050423/2120

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
			<p>either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>		
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ISR_-050423/2121

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
			underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ISR_-050423/2122
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software,	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a>	H-CIS-ISR_-050423/2123

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
			<p>Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	asaftdios-dhcpv6-cli-Zf3zTv	

**Product: isr\_1109**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-</a></p>	H-CIS-ISR_-050423/2124
-----	-------------	-----	---	--	------------------------

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
			<p>privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	sdwan-VQAHEjYw	
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ISR_-050423/2125

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
			<p>application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-ISR_-050423/2126

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ISR_050423/2127
<b>Product: isr_1109-2p</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-ISR_050423/2128

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
			<p>authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhejYw</p>	
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a></p>	H-CIS-ISR_-050423/2129

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
			<p>affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-ISR_050423/2130

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
			<p>UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ISR_050423/2131

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
<b>Product: isr_1109-4p</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw</a></p>	H-CIS-ISR_-050423/2132
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<p><a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a></p>	H-CIS-ISR_-050423/2133

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-ISR_-050423/2134</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ISR_050423/2135

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: isr_1111x</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ISR_-050423/2136
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-</a>	H-CIS-ISR_-050423/2137

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
			<p>UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ISR_-050423/2138

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
			<p>messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: isr\_1111x-8p**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ISR-050423/2139
-----	-------------	-----	--	--	-----------------------

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
			<b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ISR_050423/2140
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ISR_050423/2141

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
			<p>unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: isr_111x</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ISR_-050423/2142

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
			<p>logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ISR_050423/2143

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ISR_050423/2144
<b>Product: isr_1120</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an</p>	<a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a>	H-CIS-ISR_050423/2145

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
			<p>authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhejYw</p>	
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a></p>	H-CIS-ISR_-050423/2146

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
			<p>affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-ISR_050423/2147

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
			<p>UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ISR_050423/2148

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
<b>Product: isr_1131</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw</a></p>	H-CIS-ISR_-050423/2149
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of</p>	<p><a href="https://sec.cloudapps.cisco.com/s">https://sec.cloudapps.cisco.com/s</a></p>	H-CIS-ISR_-050423/2150

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
			<p>Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>ecurity/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
<p>Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')</p>	<p>23-Mar-2023</p>	<p>6.5</p>	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a></p>	<p>H-CIS-ISR_-050423/2151</p>

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
			<p>mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ISR_050423/2152

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
			DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: isr_1160</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts,	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw</a>	H-CIS-ISR_-050423/2153

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
			see the Details section of this advisory. <b>CVE ID : CVE-2023-20035</b>		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ISR_-050423/2154
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ISR_-050423/2155

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
			<p>this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ISR_-050423/2156

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
			device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: isr_4000</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ISR_-050423/2157
Improper Limitation	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE	<a href="https://sec.cloudapps.c">https://sec.cloudapps.c</a>	H-CIS-ISR_-050423/2158

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
of a Pathname to a Restricted Directory ('Path Traversal')			Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ISR_-050423/2159

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
			<p>device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: isr\_4221**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sdwan-VQAhEjYw</a></p>	H-CIS-ISR_-050423/2160
-----	-------------	-----	--	--	------------------------

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
			<p>shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>		
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ISR_-050423/2161

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
			system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-ISR_-050423/2162
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-</a>	H-CIS-ISR_-050423/2163

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
			<p>Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	dhcpx6-cl-Zf3zTv	

**Product: isr\_4321**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw</a></p>	H-CIS-ISR_-050423/2164
-----	-------------	-----	---	--	------------------------

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
			<p>commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>		
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ISR_-050423/2165

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
			successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem. <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ISR_-050423/2166
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	H-CIS-ISR_-050423/2167

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
			<p>Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<a href="https://content/CiscoSecurityAdvisory/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">ter/content/CiscoSecurityAdvisory/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	
<b>Product: isr_4331</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor</a>	H-CIS-ISR_-050423/2168

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
			<p>vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	y/cisco-sa-ios-xe-sdwan-VQAhejYw	
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application.</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ISR_-050423/2169

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
			<p>An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a></p>	H-CIS-ISR_-050423/2170

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
			<b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ISR_050423/2171
<b>Product: isr_4351</b>					
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	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhejYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhejYw</a>	H-CIS-ISR_-050423/2172
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content">https://sec.cloudapps.cisco.com/security/center/content</a>	H-CIS-ISR_-050423/2173

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
			<p>authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-pthtrves7GSb9V</a></p>	H-CIS-ISR_-050423/2174

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
			located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>		
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ISR_050423/2175

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
			man-in-the-middle position. <b>CVE ID : CVE-2023-20081</b>		
<b>Product: isr_4431</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw</a>	H-CIS-ISR_-050423/2176

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
			<b>CVE ID : CVE-2023-20035</b>		
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ISR_-050423/2177
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	H-CIS-ISR_-050423/2178

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
			<p>to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ISR_050423/2179

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
			<p>condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: isr_4451</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw</a></p>	H-CIS-ISR_-050423/2180

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
			system. Note: For additional information about specific impacts, see the Details section of this advisory. <b>CVE ID : CVE-2023-20035</b>		
N/A	23-Mar-2023	7.8	A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges. <b>CVE ID : CVE-2023-20065</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a>	H-CIS-ISR_050423/2181
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-</a>	H-CIS-ISR_050423/2182

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
			<p>due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ISR_050423/2183

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
			<p>device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: isr_4451-x</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw</a></p>	H-CIS-ISR_-050423/2184

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
			<p>privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>		
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ISR_-050423/2185
Improper Limitation of a Pathname to a	23-Mar-2023	6.5	<p>A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content">https://sec.cloudapps.cisco.com/security/center/content</a></p>	H-CIS-ISR_-050423/2186

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
Restricted Directory ('Path Traversal')			<p>directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>	/CiscoSecurityAdvisory/cisco-sa-webui-pthtrv-es7GSb9V	
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthdi-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafthdi-dhcpv6-cli-Zf3zTv</a></p>	H-CIS-ISR_-050423/2187

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
			<p>messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Product: isr\_4461**

Affected Version(s): -

N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAHEjYw</a></p>	H-CIS-ISR_-050423/2188
-----	-------------	-----	---	--	------------------------

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
			<p>successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>		
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	H-CIS-ISR_-050423/2189

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 Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.  <b>CVE ID : CVE-2023-20066</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrv-es7GSb9V</a>	H-CIS-ISR_-050423/2190
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	H-CIS-ISR_-050423/2191

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
			<p>of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		

**Vendor: dek-1705\_project**

**Product: dek-1705**

Affected Version(s): -

Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Mar-2023	9.8	<p>DEK-1705 &lt;=Firmware:34.23.1 device was discovered to have a command execution vulnerability.</p> <p><b>CVE ID : CVE-2023-23149</b></p>	N/A	H-DEK-DEK--050423/2192
---	-------------	-----	--	-----	------------------------

**Vendor: Dell**

**Product: embedded\_box\_pc\_3000**

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
Improper Input Validation	16-Mar-2023	6.7	Dell BIOS contains an Improper Input Validation vulnerability. A local authenticated malicious user with administrator privileges could potentially exploit this vulnerability to perform arbitrary code execution.  <b>CVE ID : CVE-2023-24571</b>	<a href="https://www.dell.com/support/kbdoc/en-us/000210955/dsa-2023-046">https://www.dell.com/support/kbdoc/en-us/000210955/dsa-2023-046</a>	H-DEL-EMBE-050423/2193
<b>Vendor: Dlink</b>					
<b>Product: dir820la1</b>					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Mar-2023	9.8	OS Command injection vulnerability in D-Link DIR820LA1_FW105B03 allows attackers to escalate privileges to root via a crafted payload with the ping_addr parameter to ping.ccp.  <b>CVE ID : CVE-2023-25280</b>	<a href="https://www.dlink.com/en/security-bulletin/">https://www.dlink.com/en/security-bulletin/</a>	H-DLI-DIR8-050423/2194
Out-of-bounds Write	16-Mar-2023	7.5	A stack overflow vulnerability exists in pingV4Msg component in D-Link DIR820LA1_FW105B03, allows attackers to cause a denial of service via the nextPage parameter to ping.ccp.  <b>CVE ID : CVE-2023-25281</b>	<a href="https://www.dlink.com/en/security-bulletin/">https://www.dlink.com/en/security-bulletin/</a>	H-DLI-DIR8-050423/2195
<b>Vendor: higa</b>					
<b>Product: powerstation</b>					
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
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Mar-2023	8.8	HGiga PowerStation remote management function has insufficient filtering for user input. An authenticated remote attacker with general user privilege can exploit this vulnerability to inject and execute arbitrary system commands to perform arbitrary system operation or disrupt service.  <b>CVE ID : CVE-2023-24837</b>	<a href="https://www.twcert.org.tw/tw/cp-132-6956-fbd85-1.html">https://www.twcert.org.tw/tw/cp-132-6956-fbd85-1.html</a>	H-HGI-POWE-050423/2196
Missing Authentication for Critical Function	27-Mar-2023	7.5	HGiga PowerStation has a vulnerability of Information Leakage. An unauthenticated remote attacker can exploit this vulnerability to obtain the administrator's credential, resulting in performing arbitrary system operation or disrupt service.  <b>CVE ID : CVE-2023-24838</b>	<a href="https://www.twcert.org.tw/tw/cp-132-6957-d8f67-1.html">https://www.twcert.org.tw/tw/cp-132-6957-d8f67-1.html</a>	H-HGI-POWE-050423/2197
<b>Vendor: hpe</b>					
<b>Product: apollo_4200_gen10_plus_system</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-APOL-050423/2198

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
			vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: apollo_4200_gen10_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbh04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbh04456en_us</a>	H-HPE-APOL-050423/2199
<b>Product: apollo_4200_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbh04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbh04456en_us</a>	H-HPE-APOL-050423/2200
<b>Product: apollo_4510_gen10_system</b>					
Affected Version(s): -					
Improper Neutralization	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability	<a href="https://support.hpe.com">https://support.hpe.com</a>	H-HPE-APOL-050423/2201

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
ion of Input During Web Page Generation ('Cross-site Scripting')			was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	m/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	
<b>Product: apollo_6500_gen10_plus_system</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-APOL-050423/2202
<b>Product: apollo_6500_gen10_system</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-APOL-050423/2203

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
			vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: apollo_n2600_gen10_plus</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbh04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbh04456en_us</a>	H-HPE-APOL-050423/2204
<b>Product: apollo_n2800_gen10_plus</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbh04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbh04456en_us</a>	H-HPE-APOL-050423/2205
<b>Product: apollo_r2000_chassis</b>					
Affected Version(s): -					
Improper Neutralization	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability	<a href="https://support.hpe.com">https://support.hpe.com</a>	H-HPE-APOL-050423/2206

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
ion of Input During Web Page Generation ('Cross-site Scripting')			was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	m/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us	
<b>Product: apollo_r2200_gen10</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-APOL-050423/2207
<b>Product: apollo_r2600_gen10</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-APOL-050423/2208

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
			vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: apollo_r2800_gen10</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbh04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbh04456en_us</a>	H-HPE-APOL-050423/2209
<b>Product: aruba_cx_10000-48y6</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2210
<b>Product: aruba_cx_6200f_48g</b>					
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-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2211
<b>Product: aruba_cx_6200m_24g</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2212
<b>Product: aruba_cx_6300m_24p</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine.	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-</a>	H-HPE-ARUB-050423/2213

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
			Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	PSA-2023-004.txt	
<b>Product: aruba_cx_6300m_48g</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2214
<b>Product: aruba_cx_6405</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2215

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
			underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>		
<b>Product: aruba_cx_6410</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2216
<b>Product: aruba_cx_8320-32</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX.	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2217

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
			<b>CVE ID : CVE-2023-1168</b>		
<b>Product: aruba_cx_8320-48p</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2218
<b>Product: aruba_cx_8325-32c</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2219
<b>Product: aruba_cx_8325-48y8c</b>					
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-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2220
<b>Product: aruba_cx_8360-12c</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2221
<b>Product: aruba_cx_8360-16y2c</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine.	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-</a>	H-HPE-ARUB-050423/2222

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
			Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	PSA-2023-004.txt	
<b>Product: aruba_cx_8360-24xf2c</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2223
<b>Product: aruba_cx_8360-32y4c</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2224

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
			underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>		
<b>Product: aruba_cx_8360-48xt4c</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2225
<b>Product: aruba_cx_8360-48y6c</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX.	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2226

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
			<b>CVE ID : CVE-2023-1168</b>		
<b>Product: aruba_cx_8400</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2227
<b>Product: aruba_cx_9300_32d</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	H-HPE-ARUB-050423/2228
<b>Product: edgeline_e920d_server_blade</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-EDGE-050423/2229
<b>Product: edgeline_e920t_server_blade</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-EDGE-050423/2230
<b>Product: edgeline_e920t_server_blade</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-EDGE-050423/2231

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_bl420c_gen8_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2232
<b>Product: proliant_bl460c_gen10_server_blade</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2233
<b>Product: proliant_bl460c_gen8_server_blade</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2234
<b>Product: proliant_bl460c_gen9_server_blade</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2235
<b>Product: proliant_bl465c_gen8_server_blade</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2236

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_bl660c_gen8_server_blade</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2237
<b>Product: proliant_bl660c_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2238
<b>Product: proliant_dl120_gen10_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-PROL-050423/2239
<b>Product: proliant_dl120_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-PROL-050423/2240
<b>Product: proliant_dl160_gen10_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-PROL-050423/2241

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_dl160_gen8_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2242
<b>Product: proliant_dl160_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2243
<b>Product: proliant_dl180_gen10_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2244
<b>Product: proliant_dl180_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2245
<b>Product: proliant_dl20_gen10_plus_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2246

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_dl20_gen10_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2247
<b>Product: proliant_dl20_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2248
<b>Product: proliant_dl320e_gen8_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2249
<b>Product: proliant_dl320e_gen8_v2_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2250
<b>Product: proliant_dl320_gen11_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2251

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_dl325_gen10_plus_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2252
<b>Product: proliant_dl325_gen10_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2253
<b>Product: proliant_dl325_gen11_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2254
<b>Product: proliant_dl345_gen10_plus_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2255
<b>Product: proliant_dl345_gen11_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2256

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_dl360e_gen8_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2257
<b>Product: proliant_dl360p_gen8_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2258
<b>Product: proliant_dl360_gen10_plus_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-PROL-050423/2259
<b>Product: proliant_dl360_gen10_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-PROL-050423/2260
<b>Product: proliant_dl360_gen11_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-PROL-050423/2261

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_dl360_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2262
<b>Product: proliant_dl365_gen10_plus_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2263
<b>Product: proliant_dl365_gen11_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-PROL-050423/2264
<b>Product: proliant_dl380e_gen8_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-PROL-050423/2265
<b>Product: proliant_dl380p_gen8_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-PROL-050423/2266

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_dl380_gen10_plus_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2267
<b>Product: proliant_dl380_gen10_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2268
<b>Product: proliant_dl380_gen11_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2269
<b>Product: proliant_dl380_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2270
<b>Product: proliant_dl385p_gen8_(amd\)</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2271

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_dl385_gen10_plus_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2272
<b>Product: proliant_dl385_gen10_plus_v2_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2273
<b>Product: proliant_dl385_gen10_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2274
<b>Product: proliant_dl385_gen11_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2275
<b>Product: proliant_dl560_gen10_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2276

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_dl560_gen8_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2277
<b>Product: proliant_dl560_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2278
<b>Product: proliant_dl580_gen10_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2279
<b>Product: proliant_dl580_gen8_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2280
<b>Product: proliant_dl580_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2281

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_dl60_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2282
<b>Product: proliant_dl80_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2283
<b>Product: proliant_dx170r_gen10_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2284
<b>Product: proliant_dx190r_gen10_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2285
<b>Product: proliant_dx220n_gen10_plus_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2286

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_dx325_gen10_plus_v2_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2287
<b>Product: proliant_dx360_gen10_plus_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2288
<b>Product: proliant_dx360_gen10_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2289
<b>Product: proliant_dx380_gen10_plus_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2290
<b>Product: proliant_dx380_gen10_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2291

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_dx385_gen10_plus_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2292
<b>Product: proliant_dx385_gen10_plus_v2_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2293
<b>Product: proliant_dx4200_gen10_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2294
<b>Product: proliant_dx560_gen10_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2295
<b>Product: proliant_e910t_server_blade</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2296

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_e910_server_blade</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2297
<b>Product: proliant_microserver_gen8</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2298
<b>Product: proliant_ml110_gen10_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2299
<b>Product: proliant_ml110_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2300
<b>Product: proliant_ml30_gen10_plus_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2301

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_ml30_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2302
<b>Product: proliant_ml310e_gen8_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2303
<b>Product: proliant_ml310e_gen8_v2_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2304
<b>Product: proliant_ml350e_gen8_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2305
<b>Product: proliant_ml350e_gen8_v2_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2306

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_ml350p_gen8_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2307
<b>Product: proliant_ml350_gen10_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2308
<b>Product: proliant_ml350_gen11_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2309
<b>Product: proliant_ml350_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2310
<b>Product: proliant_sl210t_gen8_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2311

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_sl230s_gen8_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2312
<b>Product: proliant_sl250s_gen8_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2313
<b>Product: proliant_sl270s_gen8_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2314
<b>Product: proliant_sl270s_gen8_se_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2315
<b>Product: proliant_ws460c_gen8_graphics_server_blade</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2316

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_ws460c_gen9_graphics_server_blade</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2317
<b>Product: proliant_xl170r_gen10_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2318
<b>Product: proliant_xl170r_gen9_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out.  <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-PROL-050423/2319
<b>Product: proliant_xl190r_gen10_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out.  <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-PROL-050423/2320
<b>Product: proliant_xl190r_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-PROL-050423/2321

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_xl220a_gen8_v2_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2322
<b>Product: proliant_xl220n_gen10_plus_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2323
<b>Product: proliant_xl225n_gen10_plus_1u_node</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2324
<b>Product: proliant_xl230a_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2325
<b>Product: proliant_xl230b_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2326

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_xl230k_gen10_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-PROL-050423/2327
<b>Product: proliant_xl250a_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-PROL-050423/2328
<b>Product: proliant_xl270d_gen10_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2329
<b>Product: proliant_xl270d_gen9_special_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2330
<b>Product: proliant_xl290n_gen10_plus_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2331

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_xl450_gen10_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2332
<b>Product: proliant_xl450_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2333
<b>Product: proliant_xl645d_gen10_plus_server</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2334
<b>Product: proliant_xl675d_gen10_plus_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2335
<b>Product: proliant_xl730f_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2336

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: proliant_xl740f_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2337
<b>Product: proliant_xl750f_gen9_server</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-PROL-050423/2338
<b>Product: storage_file_controller</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-STOR-050423/2339
<b>Product: storage_performance_file_controller</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-STOR-050423/2340
<b>Product: storeeasy_1430_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpeshbf04456en_us</a>	H-HPE-STOR-050423/2341

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: storeeasy_1440_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2342
<b>Product: storeeasy_1450_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2343
<b>Product: storeeasy_1460_storage</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2344
<b>Product: storeeasy_1530_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2345
<b>Product: storeeasy_1540_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2346

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: storeeasy_1550_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2347
<b>Product: storeeasy_1560_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2348
<b>Product: storeeasy_1630_storage</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2349
<b>Product: storeeasy_1640_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2350
<b>Product: storeeasy_1650_expanded_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2351

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: storeeasy_1650_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2352
<b>Product: storeeasy_1660_expanded_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2353
<b>Product: storeeasy_1660_performance_storage</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2354
<b>Product: storeeasy_1660_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2355
<b>Product: storeeasy_1830_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2356

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: storeeasy_1840_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2357
<b>Product: storeeasy_1850_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2358
<b>Product: storeeasy_1860_performance_storage</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2359
<b>Product: storeeasy_1860_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2360
<b>Product: storeeasy_3830_gateway_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2361

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: storeeasy_3830_gateway_storage_blade</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2362
<b>Product: storeeasy_3840_gateway_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2363
<b>Product: storeeasy_3840_gateway_storage_blade</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2364
<b>Product: storeeasy_3850_gateway_single_node_upgrade</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2365
<b>Product: storeeasy_3850_gateway_storage</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2366

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: storeeasy_3850_gateway_storage_blade</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2367
<b>Product: storevirtual_3000_file_controller</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-STOR-050423/2368
<b>Product: synergy_480_gen10_compute_module</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-SYNE-050423/2369
<b>Product: synergy_480_gen10_plus_compute_module</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-SYNE-050423/2370
<b>Product: synergy_480_gen9_compute_module</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-SYNE-050423/2371

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
			updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>		
<b>Product: synergy_620_gen9_compute_module</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-SYNE-050423/2372
<b>Product: synergy_660_gen10_compute_module</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpsc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-SYNE-050423/2373
<b>Product: synergy_660_gen9_compute_module</b>					
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
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-SYNE-050423/2374
<b>Product: synergy_680_gen9_compute_module</b>					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	H-HPE-SYNE-050423/2375
<b>Vendor: jcgcn.com</b>					
<b>Product: jhr-n916r</b>					
Affected Version(s): -					
N/A	16-Mar-2023	9.8	Command execution vulnerability was discovered in JHR-N916R router firmware version<=21.11.1.1483. <b>CVE ID : CVE-2023-24795</b>	N/A	H-JCG-JHR--050423/2376

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
<b>Vendor: lancombg</b>					
<b>Product: sa-wr915nd</b>					
Affected Version(s): -					
N/A	16-Mar-2023	9.8	SA-WR915ND router firmware v17.35.1 was discovered to be vulnerable to code execution. <b>CVE ID : CVE-2023-23150</b>	N/A	H-LAN-SA-W-050423/2377
<b>Vendor: Omron</b>					
<b>Product: sysmac_cj2h-cpu64</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2378
<b>Product: sysmac_cj2h-cpu64-eip</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where	<a href="https://www.ia.omron.com/product/vulnera">https://www.ia.omron.com/product/vulnera</a>	H-OMR-SYSM-050423/2379

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
			<p>the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program.</p> <p><b>CVE ID : CVE-2023-0811</b></p>	<p>bility/OMS R-2023-001_en.pdf</p>	

**Product: sysmac\_cj2h-cpu65**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	<p>Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program.</p> <p><b>CVE ID : CVE-2023-0811</b></p>	<p><a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a></p>	H-OMR-SYSM-050423/2380
-------------------------	-------------	-----	--	--	------------------------

**Product: sysmac\_cj2h-cpu65-eip**

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): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2381

**Product: sysmac\_cj2h-cpu66**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2382
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cj2h-cpu66-eip</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2383
<b>Product: sysmac_cj2h-cpu67</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2384

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cj2h-cpu67-eip**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2385
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cj2h-cpu68**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2386
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cj2h-cpu68-eip**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2387
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cj2m-cpu11**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	H-OMR-SYSM-050423/2388
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cj2m-cpu12**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2389
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cj2m-cpu13**

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): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2390

**Product: sysmac\_cj2m-cpu14**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2391
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cj2m-cpu15</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2392
<b>Product: sysmac_cj2m-cpu31</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2393

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cj2m-cpu32**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2394
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cj2m-cpu33**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2395
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cj2m-cpu34**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2396
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cj2m-cpu35**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	H-OMR-SYSM-050423/2397
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp1e-e10dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2398
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1e-e10dr-d**

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): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2399
<b>Product: sysmac_cp1e-e10dt-a</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2400

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp1e-e10dt-d</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2401
<b>Product: sysmac_cp1e-e10dt1-a</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2402

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1e-e10dt1-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2403
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1e-e14dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2404
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1e-e14sdr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2405
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1e-e20dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	H-OMR-SYSM-050423/2406
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp1e-e20sdr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2407
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1e-e30dr-a**

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): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2408

**Product: sysmac\_cp1e-e30sdr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2409
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp1e-e40dr-a</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2410
<b>Product: sysmac_cp1e-e40sdr-a</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2411

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1e-e60sdr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2412
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1e-na20dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2413
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1e-na20dt-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2414
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1e-na20dt1-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	H-OMR-SYSM-050423/2415
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp1h-x40dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2416
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1h-x40dt-d**

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): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2417

**Product: sysmac\_cp1h-x40dt1-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2418
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp1h-xa40dr-a</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2419
<b>Product: sysmac_cp1h-xa40dt-d</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2420

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1h-xa40dt1-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2421
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1h-y20dt-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2422
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp11-el20dr-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2423
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp11-em30dr-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	H-OMR-SYSM-050423/2424
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp1l-em30dt-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2425
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1l-em30dt1-d**

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): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2426
<b>Product: sysmac_cp1l-em40dr-d</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2427

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp1l-em40dt-d</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2428
<b>Product: sysmac_cp1l-em40dt1-d</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2429

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1l-l10dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2430
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1l-l10dr-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2431
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1l-l10dt-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2432
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1l-l10dt-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	H-OMR-SYSM-050423/2433
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp1l-l10dt1-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2434
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1l-l14dr-a**

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): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2435

**Product: sysmac\_cp1l-l14dr-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2436
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp1l-l14dt-a</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2437
<b>Product: sysmac_cp1l-l14dt-d</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2438

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp11-l14dt1-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2439
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp11-l20dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2440
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp11-l20dr-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2441
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp11-l20dt-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	H-OMR-SYSM-050423/2442
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp11-l20dt-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2443
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp11-l20dt1-d**

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): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2444

**Product: sysmac\_cp1l-m30dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2445
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp1l-m30dr-d</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2446
<b>Product: sysmac_cp1l-m30dt-a</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2447

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp11-m30dt-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2448
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp11-m30dt1-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2449
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp11-m40dr-a</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2450
<b>Product: sysmac_cp11-m40dr-d</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	H-OMR-SYSM-050423/2451

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp1l-m40dt-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2452
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1l-m40dt-d**

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): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2453

**Product: sysmac\_cp1l-m40dt1-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2454
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp1l-m60dr-a</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2455
<b>Product: sysmac_cp1l-m60dr-d</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2456

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1l-m60dt-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2457
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1l-m60dt-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2458
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp11-m60dt1-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2459
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-e14dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	H-OMR-SYSM-050423/2460
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp2e-e20dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2461
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-e30dr-a**

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): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2462

**Product: sysmac\_cp2e-e40dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2463
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp2e-e60dr-a</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2464
<b>Product: sysmac_cp2e-n14dr-a</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2465

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp2e-n14dr-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2466
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n14dt-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2467
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp2e-n14dt-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2468
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n14dt1-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	H-OMR-SYSM-050423/2469
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp2e-n20dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2470
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n20dr-d**

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): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2471

**Product: sysmac\_cp2e-n20dt-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2472
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp2e-n20dt-d</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2473
<b>Product: sysmac_cp2e-n20dt1-d</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2474

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp2e-n30dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2475
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n30dr-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2476
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp2e-n30dt-a</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2477
<b>Product: sysmac_cp2e-n30dt-d</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	H-OMR-SYSM-050423/2478

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp2e-n30dt1-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2479
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n40dr-a**

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): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2480

**Product: sysmac\_cp2e-n40dr-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2481
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp2e-n40dt-a</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2482
<b>Product: sysmac_cp2e-n40dt-d</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2483

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp2e-n40dt1-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2484
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n60dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2485
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp2e-n60dr-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2486
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n60dt-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	H-OMR-SYSM-050423/2487
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp2e-n60dt-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2488
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n60dt1-d**

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): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2489

**Product: sysmac\_cp2e-s30dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2490
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp2e-s30dt-d</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2491
<b>Product: sysmac_cp2e-s30dt1-d</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2492

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp2e-s40dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2493
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-s40dt-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2494
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp2e-s40dt1-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2495
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-s60dr-a**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	H-OMR-SYSM-050423/2496
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp2e-s60dt-d**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2497
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-s60dt1-d**

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): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2498

**Product: sysmac\_cs1w-drm21-v1**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2499
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cs1w-eip21</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2500
<b>Product: sysmac_cs1w-etn21</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2501

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cs1w-fln22**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2502
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cs1w-nc\[\]71**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2503
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cs1w-spu01-v2**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	H-OMR-SYSM-050423/2504
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cs1w-spu02-v2**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	H-OMR-SYSM-050423/2505
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	
<b>Vendor: paradox</b>					
<b>Product: ipr512</b>					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	21-Mar-2023	7.5	An issue found in Paradox Security Systems IPR512 allows attackers to cause a denial of service via the login.html and login.xml parameters. <b>CVE ID : CVE-2023-24709</b>	N/A	H-PAR-IPR5-050423/2506
<b>Vendor: Samsung</b>					
<b>Product: exynos</b>					
Affected Version(s): -					
N/A	16-Mar-2023	9.1	Improper authorization implementation in Exynos baseband prior to SMR Mar-2023 Release 1 allows incorrect handling of unencrypted message.	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=20">https://security.samsungmobile.com/securityUpdate.smb?year=20</a>	H-SAM-EXYN-050423/2507

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
			<b>CVE ID : CVE-2023-21455</b>	23&month=03	
<b>Product: exynos_1080</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fntp attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26496</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	H-SAM-EXYN-050423/2508
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute. <b>CVE ID : CVE-2023-26497</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	H-SAM-EXYN-050423/2509
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos	<a href="https://semiconductor.samsung.com/support/quality-support/pr">https://semiconductor.samsung.com/support/quality-support/pr</a>	H-SAM-EXYN-050423/2510

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
			1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26498</b>	oduct-security-updates/	
<b>Product: exynos_2100</b>					
Affected Version(s): -					
Use After Free	16-Mar-2023	9.8	Use after free vulnerability in decon driver prior to SMR Mar-2023 Release 1 allows attackers to cause memory access fault. <b>CVE ID : CVE-2023-21459</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	H-SAM-EXYN-050423/2511
<b>Product: exynos_980</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fntp attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26496</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	H-SAM-EXYN-050423/2512

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute.  <b>CVE ID : CVE-2023-26497</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	H-SAM-EXYN-050423/2513
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module.  <b>CVE ID : CVE-2023-26498</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	H-SAM-EXYN-050423/2514
<b>Product: exynos_auto_t5123</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	H-SAM-EXYN-050423/2515

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
			corruption can occur due to improper checking of the parameter length while parsing the fntp attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26496</b>	security-updates/	
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute. <b>CVE ID : CVE-2023-26497</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	H-SAM-EXYN-050423/2516
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26498</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	H-SAM-EXYN-050423/2517

**Product: exynos\_modem\_5123**

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): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fmtp attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26496</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	H-SAM-EXYN-050423/2518
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute. <b>CVE ID : CVE-2023-26497</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	H-SAM-EXYN-050423/2519
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	H-SAM-EXYN-050423/2520

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26498</b>		
<b>Product: exynos_modem_5300</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fntp attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26496</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	H-SAM-EXYN-050423/2521
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute.	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	H-SAM-EXYN-050423/2522

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
			<b>CVE ID : CVE-2023-26497</b>		
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26498</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	H-SAM-EXYN-050423/2523

**Vendor: sauter-controls**

**Product: ey-as525f001**

Affected Version(s): -

Cleartext Transmission of Sensitive Information	27-Mar-2023	6.5	An authenticated malicious user could acquire the simple mail transfer protocol (SMTP) Password in cleartext format, despite it being protected and hidden behind asterisks. The attacker could then perform further attacks using the SMTP credentials. <b>CVE ID : CVE-2023-27927</b>	N/A	H-SAU-EY-A-050423/2524
Unrestricted Upload of File with Dangerous Type	27-Mar-2023	6.5	An authenticated malicious user could successfully upload a malicious image could	N/A	H-SAU-EY-A-050423/2525

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
			lead to a denial-of-service condition. <b>CVE ID : CVE-2023-28652</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	An unauthenticated remote attacker could force all authenticated users, such as administrative users, to perform unauthorized actions by viewing the logs. This action would also grant the attacker privilege escalation. <b>CVE ID : CVE-2023-22300</b>	N/A	H-SAU-EY-A-050423/2526
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	An unauthenticated remote attacker could provide a malicious link and trick an unsuspecting user into clicking on it. If clicked, the attacker could execute the malicious JavaScript (JS) payload in the target's security context. <b>CVE ID : CVE-2023-28650</b>	N/A	H-SAU-EY-A-050423/2527
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	5.4	A malicious user could leverage this vulnerability to escalate privileges or perform unauthorized actions in the context of the targeted privileged users. <b>CVE ID : CVE-2023-28655</b>	N/A	H-SAU-EY-A-050423/2528
<b>Vendor: silabs</b>					
<b>Product: wireless_smart_ubiquitous_network_linux_border_router</b>					
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
Missing Authorization	21-Mar-2023	5.3	Missing MAC layer security in Silicon Labs Wi-SUN Linux Border Router v1.5.2 and earlier allows malicious node to route malicious messages through network. <b>CVE ID : CVE-2023-1262</b>	N/A	H-SIL-WIRE-050423/2529
<b>Vendor: Tenda</b>					
<b>Product: ax3</b>					
Affected Version(s): -					
Out-of-bounds Write	24-Mar-2023	8.8	Tenda AX3 V16.03.12.11 is vulnerable to Buffer Overflow via /goform/SetFirewallCfg. <b>CVE ID : CVE-2023-27042</b>	N/A	H-TEN-AX3-050423/2530
<b>Product: g103</b>					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Mar-2023	7.5	Command Injection vulnerability found in Tenda G103 v.1.0.05 allows an attacker to obtain sensitive information via a crafted package <b>CVE ID : CVE-2023-27079</b>	N/A	H-TEN-G103-050423/2531
<b>Product: w20e</b>					
Affected Version(s): -					
Out-of-bounds Write	19-Mar-2023	9.8	Tenda W20E v15.11.0.6 (US_W20EV4.0br_v15.11.0.6(1068_1546_841)_CN_TDC) is vulnerable to Buffer Overflow via function formIPMacBindModify.	N/A	H-TEN-W20E-050423/2532

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
			<b>CVE ID : CVE-2023-26805</b>		
Out-of-bounds Write	19-Mar-2023	9.8	Tenda W20E v15.11.0.6(US_W20EV4.0 br_v15.11.0.6(1068_1546_841 is vulnerable to Buffer Overflow via function formSetSysTime, <b>CVE ID : CVE-2023-26806</b>	N/A	H-TEN-W20E-050423/2533
<b>Vendor: totolink</b>					
<b>Product: a7100ru</b>					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Mar-2023	9.8	TOTOLink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the enabled parameter at /setting/setWanIeCfg. <b>CVE ID : CVE-2023-27135</b>	N/A	H-TOT-A710-050423/2534
<b>Vendor: Tp-link</b>					
<b>Product: tl-mr3020</b>					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Mar-2023	9.8	A command injection issue was found in TP-Link MR3020 v.1_150921 that allows a remote attacker to execute arbitrary commands via a crafted request to the tftp endpoint. <b>CVE ID : CVE-2023-27078</b>	N/A	H-TP--TL-M-050423/2535
<b>Vendor: ui</b>					
<b>Product: edgerouter_x</b>					
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
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in Ubiquiti EdgeRouter X 2.0.9-hotfix.6. This issue affects some unknown processing of the component NAT Configuration Handler. The manipulation leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. The identifier VDB-223301 was assigned to this vulnerability. NOTE: The vendor position is that post-authentication issues are not accepted as vulnerabilities. <b>CVE ID : CVE-2023-1456</b>	N/A	H-UI-EDGE-050423/2536
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Mar-2023	9.8	<b>** DISPUTED **</b> A vulnerability, which was classified as critical, was found in Ubiquiti EdgeRouter X 2.0.9-hotfix.6. Affected is an unknown function of the component Static Routing Configuration Handler. The manipulation of the argument next-hop-interface leads to command injection. It is possible to launch the attack remotely. The exploit has been	N/A	H-UI-EDGE-050423/2537

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
			disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. VDB-223302 is the identifier assigned to this vulnerability. NOTE: The vendor position is that post-authentication issues are not accepted as vulnerabilities. <b>CVE ID : CVE-2023-1457</b>		
<b>Operating System</b>					
<b>Vendor: 360</b>					
<b>Product: d901_firmware</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	7.5	Stack Overflow vulnerability found in 360 D901 allows a remote attacker to cause a Distributed Denial of Service (DDOS) via a crafted HTTP package. <b>CVE ID : CVE-2023-27077</b>	N/A	O-360-D901-050423/2538
<b>Vendor: Apple</b>					
<b>Product: macos</b>					
Affected Version(s): -					
Improper Input Validation	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	<a href="https://helpx.adobe.com/security/products/illustrator/psb23-19.html">https://helpx.adobe.com/security/products/illustrator/psb23-19.html</a>	O-APP-MACO-050423/2539

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
			victim must open a malicious file. <b>CVE ID : CVE-2023-25859</b>		
Integer Overflow or Wraparound	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-25903</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	O-APP-MACO-050423/2540
Access of Uninitialized Pointer	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26334</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	O-APP-MACO-050423/2541
Out-of-bounds Read	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	O-APP-MACO-050423/2542

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
			<p>allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p><b>CVE ID : CVE-2023-26335</b></p>		
Use After Free	28-Mar-2023	7.8	<p>Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p><b>CVE ID : CVE-2023-26336</b></p>	<p><a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a></p>	O-APP-MACO-050423/2543
Out-of-bounds Write	28-Mar-2023	7.8	<p>Adobe Dimension versions 3.4.7 (and earlier) is affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p><b>CVE ID : CVE-2023-26337</b></p>	<p><a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a></p>	O-APP-MACO-050423/2544

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26338</b>	<a href="https://helpx.adobe.com/security/products/dimension/psb23-20.html">https://helpx.adobe.com/security/products/dimension/psb23-20.html</a>	O-APP-MACO-050423/2545
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26339</b>	<a href="https://helpx.adobe.com/security/products/dimension/psb23-20.html">https://helpx.adobe.com/security/products/dimension/psb23-20.html</a>	O-APP-MACO-050423/2546
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to	<a href="https://helpx.adobe.com/security/products/dimension/psb23-20.html">https://helpx.adobe.com/security/products/dimension/psb23-20.html</a>	O-APP-MACO-050423/2547

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26340</b>		
<b>Vendor: centralite</b>					
<b>Product: pearl_firmware</b>					
Affected Version(s): 0x04075010					
N/A	17-Mar-2023	7.5	A vulnerability in Centralite Pearl Thermostat 0x04075010 allows attackers to cause a Denial of Service (DoS) via a crafted Zigbee message. <b>CVE ID : CVE-2023-24678</b>	N/A	O-CEN-PEAR-050423/2548
<b>Vendor: Cisco</b>					
<b>Product: ios</b>					
Affected Version(s): 12.2\\(6\\)i1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2549

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
			exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.1\\(2\\)sg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2550
Affected Version(s): 15.1\\(2\\)sg1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2551

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
			<p>vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	dos-44cMvdDK	
Affected Version(s): 15.1\\(2\\)sg2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2552
Affected Version(s): 15.1\\(2\\)sg3					
Improper Validation	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6	<a href="https://sec.cloudapps.c">https://sec.cloudapps.c</a>	O-CIS-IOS-050423/2553

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
of Array Index			(DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	isco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(2\\)sg4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2554

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
			device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.1\\(2\\)sg5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2555
Affected Version(s): 15.1\\(2\\)sg6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2556

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
			data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.1\\(2\\)sg7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2557
Affected Version(s): 15.1\\(2\\)sg8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	O-CIS-IOS-050423/2558

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
			<p>IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://content.cisco.com/content/cisco-security/cisco-sa-ios-dhcpv6-dos-44cMvdDK">ter/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	
Affected Version(s): 15.1\\(2\\)sy1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2559

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.1\\(2\\)sy10					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2560
Affected Version(s): 15.1\\(2\\)sy11					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2561

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.1\\(2\\)sy12					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2562
Affected Version(s): 15.1\\(2\\)sy13					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2563

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(2\\)sy14					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2564

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.1\\(2\\)sy15					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2565
Affected Version(s): 15.1\\(2\\)sy16					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2566

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.1\\(2\\)sy16a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2567
Affected Version(s): 15.1\\(2\\)sy2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2568

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(2\\)sy3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2569

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.1\\(2\\)sy4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2570
Affected Version(s): 15.1\\(2\\)sy4a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2571

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.1\\(2\\)sy5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2572
Affected Version(s): 15.1\\(2\\)sy6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2573

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(2\\)sy7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2574

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.1\\(2\\)sy8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2575
Affected Version(s): 15.1\\(2\\)sy9					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2576

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.1\\(3\\)svr10					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2577
Affected Version(s): 15.1\\(3\\)svs					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2578

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(3\\)svt1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2579

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.1\\(3\\)svt3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2580
Affected Version(s): 15.1\\(3\\)svt4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2581

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.1\\(3\\)svu1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2582
Affected Version(s): 15.1\\(3\\)svu10					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2583

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(3\\)svu11					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2584

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.1\\(3\\)svu2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2585
Affected Version(s): 15.1\\(3\\)svu20					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2586

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.1\\(3\\)svu21					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2587
Affected Version(s): 15.1\\(3\\)svv1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2588

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.1\\(3\\)svv2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2589

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.1\\(3\\)svv3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2590
Affected Version(s): 15.1\\(3\\)svw					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2591

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.1\\(3\\)svw1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2592
Affected Version(s): 15.1\\(3\\)svx					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2593

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 15.1\\(3\\)svx1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2594

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.1\\(4\\)m10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2595
Affected Version(s): 15.1\\(4\\)m12a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2596

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.1\\(4\\)m7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2597
Affected Version(s): 15.1\\(4\\)m8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2598

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 15.1\\(4\\)m9					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2599

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(1\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2600
Affected Version(s): 15.2\\(1\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2601

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(1\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2602
Affected Version(s): 15.2\\(1\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2603

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(1\\)ey					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2604

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(1\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2605
Affected Version(s): 15.2\\(1\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2606

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(1\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2607
Affected Version(s): 15.2\\(1\\)sy					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2608

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(1\\)sy0a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2609

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(1\\)sy1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2610
Affected Version(s): 15.2\\(1\\)sy1a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2611

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(1\\)sy2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2612
Affected Version(s): 15.2\\(1\\)sy3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2613

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 15.2\\(1\\)sy4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2614

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(1\\)sy5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2615
Affected Version(s): 15.2\\(1\\)sy6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2616

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(1\\)sy7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2617
Affected Version(s): 15.2\\(1\\)sy8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2618

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 15.2\\(2\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2619

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(2\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2620
Affected Version(s): 15.2\\(2\\)e10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2621

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(2\\)e10a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2622
Affected Version(s): 15.2\\(2\\)e10b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2623

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2624

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(2\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2625
Affected Version(s): 15.2\\(2\\)e4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2626

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(2\\)e5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2627
Affected Version(s): 15.2\\(2\\)e5a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2628

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2\\)e5b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2629

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(2\\)e6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2630
Affected Version(s): 15.2\\(2\\)e7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2631

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(2\\)e7b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2632
Affected Version(s): 15.2\\(2\\)e8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2633

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2\\)e9					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2634

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(2\\)e9a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2635
Affected Version(s): 15.2\\(2\\)ea					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2636

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(2\\)ea1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2637
Affected Version(s): 15.2\\(2\\)ea2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2638

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2\\)ea3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2639

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(2\\)eb					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2640
Affected Version(s): 15.2\\(2\\)eb1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2641

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(2\\)eb2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2642
Affected Version(s): 15.2\\(2\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2643

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2\\)s0a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2644

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(2\\)s0c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2645
Affected Version(s): 15.2\\(2\\)s0d					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2646

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(2\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2647
Affected Version(s): 15.2\\(2\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2648

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2\\)sc1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2649

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(2\\)sc3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2650
Affected Version(s): 15.2\\(2\\)sc4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2651

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(2\\)sy					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2652
Affected Version(s): 15.2\\(2\\)sy1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2653

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(2\\)sy2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2654

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(2\\)sy3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2655
Affected Version(s): 15.2\\(234k\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2656

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(2a\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2657
Affected Version(s): 15.2\\(2a\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2658

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 15.2\\(2b\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2659

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(3\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2660
Affected Version(s): 15.2\\(3\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2661

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(3\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2662
Affected Version(s): 15.2\\(3\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2663

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(3\\)e4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2664

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(3\\)e5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2665
Affected Version(s): 15.2\\(3\\)ea					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2666

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(3a\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2667
Affected Version(s): 15.2\\(3m\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2668

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 15.2\\(3m\\)e7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2669

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(3m\\)e8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2670
Affected Version(s): 15.2\\(4\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2671

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(4\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2672
Affected Version(s): 15.2\\(4\\)e10					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2673

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)e10a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2674

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(4\\)e10b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2675
Affected Version(s): 15.2\\(4\\)e10c					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2676

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(4\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2677
Affected Version(s): 15.2\\(4\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2678

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 15.2\\(4\\)e4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2679

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(4\\)e5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2680
Affected Version(s): 15.2\\(4\\)e5a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2681

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(4\\)e6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2682
Affected Version(s): 15.2\\(4\\)e7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2683

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)e8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2684

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(4\\)e9					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2685
Affected Version(s): 15.2\\(4\\)ea					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2686

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(4\\)ea1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2687
Affected Version(s): 15.2\\(4\\)ea2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2688

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK</p>	
Affected Version(s): 15.2\\(4\\)ea3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2689

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(4\\)ea4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2690
Affected Version(s): 15.2\\(4\\)ea5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2691

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(4\\)ea6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2692
Affected Version(s): 15.2\\(4\\)ea7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2693

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 15.2\\(4\\)ea8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2694

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(4\\)ea9					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2695
Affected Version(s): 15.2\\(4\\)ea9a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2696

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(4\\)ec1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2697
Affected Version(s): 15.2\\(4\\)ec2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2698

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)gc1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2699

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(4\\)gc2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2700
Affected Version(s): 15.2\\(4\\)gc3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2701

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(4\\)m10					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2702
Affected Version(s): 15.2\\(4\\)m11					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2703

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)m5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2704

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(4\\)m6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2705
Affected Version(s): 15.2\\(4\\)m6a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2706

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(4\\)m6b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2707
Affected Version(s): 15.2\\(4\\)m7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2708

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 15.2\\(4\\)m8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2709

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(4\\)m9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2710
Affected Version(s): 15.2\\(4\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2711

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(4\\)s0c					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2712
Affected Version(s): 15.2\\(4\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2713

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)s1c					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2714

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(4\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2715
Affected Version(s): 15.2\\(4\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2716

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(4\\)s3a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2717
Affected Version(s): 15.2\\(4\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2718

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4\\)s4a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2719

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(4\\)s5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2720
Affected Version(s): 15.2\\(4\\)s6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2721

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(4\\)s7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2722
Affected Version(s): 15.2\\(4\\)s8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2723

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 15.2\\(4m\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2724

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(4m\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2725
Affected Version(s): 15.2\\(4m\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2726

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(4n\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2727
Affected Version(s): 15.2\\(4o\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2728

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(4o\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2729

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(4p\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2730
Affected Version(s): 15.2\\(4q\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2731

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(4s\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2732
Affected Version(s): 15.2\\(5\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2733

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(5\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2734

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(5\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2735
Affected Version(s): 15.2\\(5\\)e2b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2736

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(5\\)e2c					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2737
Affected Version(s): 15.2\\(5\\)ea					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2738

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(5\\)ex					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2739

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(5a\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2740
Affected Version(s): 15.2\\(5a\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2741

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(5b\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2742
Affected Version(s): 15.2\\(5c\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2743

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(6\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2744

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(6\\)e0a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2745
Affected Version(s): 15.2\\(6\\)e0c					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2746

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(6\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2747
Affected Version(s): 15.2\\(6\\)e1a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2748

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(6\\)e1s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2749

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(6\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2750
Affected Version(s): 15.2\\(6\\)e2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2751

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(6\\)e2b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2752
Affected Version(s): 15.2\\(6\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2753

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(6\\)eb					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2754

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(7\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2755
Affected Version(s): 15.2\\(7\\)e0a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2756

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(7\\)e0b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2757
Affected Version(s): 15.2\\(7\\)e0s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2758

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(7\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2759

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(7\\)e1a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2760
Affected Version(s): 15.2\\(7\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2761

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(7\\)e2a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2762
Affected Version(s): 15.2\\(7\\)e2b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2763

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(7\\)e3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2764

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(7\\)e3a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2765
Affected Version(s): 15.2\\(7\\)e3k					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2766

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(7\\)e4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2767
Affected Version(s): 15.2\\(7\\)e5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2768

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(7\\)e6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2769

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.2\\(7a\\)e0b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2770
Affected Version(s): 15.2\\(7b\\)e0b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2771

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.2\\(8\\)e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2772
Affected Version(s): 15.2\\(8\\)e1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2773

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.2\\(8\\)e2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2774

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.3\\(0\\)sy					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2775
Affected Version(s): 15.3\\(1\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2776

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.3\\(1\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2777
Affected Version(s): 15.3\\(1\\)s1e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2778

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.3\\(1\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2779

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.3\\(1\\)sy					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2780
Affected Version(s): 15.3\\(1\\)sy1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2781

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.3\\(1\\)sy2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2782
Affected Version(s): 15.3\\(2\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2783

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.3\\(2\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2784

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.3\\(2\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2785
Affected Version(s): 15.3\\(2\\)t1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2786

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.3\\(2\\)t2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2787
Affected Version(s): 15.3\\(2\\)t3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2788

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 15.3\\(2\\)t4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2789

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.3\\(3\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2790
Affected Version(s): 15.3\\(3\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2791

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.3\\(3\\)s10					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2792
Affected Version(s): 15.3\\(3\\)s1a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2793

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 15.3\\(3\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2794

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.3\\(3\\)s2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2795
Affected Version(s): 15.3\\(3\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2796

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.3\\(3\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2797
Affected Version(s): 15.3\\(3\\)s5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2798

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.3\\(3\\)s6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2799

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.3\\(3\\)s6a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2800
Affected Version(s): 15.3\\(3\\)s7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2801

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.3\\(3\\)s8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2802
Affected Version(s): 15.3\\(3\\)s8a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2803

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 15.3\\(3\\)s9					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2804

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.4\\(1\\)cg					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2805
Affected Version(s): 15.4\\(1\\)cg1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2806

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.4\\(1\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2807
Affected Version(s): 15.4\\(1\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2808

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(1\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2809

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.4\\(1\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2810
Affected Version(s): 15.4\\(1\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2811

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.4\\(1\\)sy					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2812
Affected Version(s): 15.4\\(1\\)sy1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2813

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(1\\)sy2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2814

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.4\\(1\\)sy3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2815
Affected Version(s): 15.4\\(1\\)sy4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2816

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.4\\(1\\)t					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2817
Affected Version(s): 15.4\\(1\\)t1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2818

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(1\\)t2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2819

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.4\\(1\\)t3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2820
Affected Version(s): 15.4\\(1\\)t4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2821

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.4\\(2\\)cg					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2822
Affected Version(s): 15.4\\(2\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2823

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(2\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2824

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.4\\(2\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2825
Affected Version(s): 15.4\\(2\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2826

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.4\\(2\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2827
Affected Version(s): 15.4\\(2\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2828

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(2\\)sn1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2829

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.4\\(2\\)t					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2830
Affected Version(s): 15.4\\(2\\)t1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2831

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.4\\(2\\)t2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2832
Affected Version(s): 15.4\\(2\\)t3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2833

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(2\\)t4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2834

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.4\\(3\\)m					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2835
Affected Version(s): 15.4\\(3\\)m1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2836

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.4\\(3\\)m10					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2837
Affected Version(s): 15.4\\(3\\)m2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2838

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(3\\)m3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2839

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.4\\(3\\)m4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2840
Affected Version(s): 15.4\\(3\\)m5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2841

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.4\\(3\\)m6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2842
Affected Version(s): 15.4\\(3\\)m6a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2843

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 15.4\\(3\\)m7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2844

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.4\\(3\\)m7a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2845
Affected Version(s): 15.4\\(3\\)m8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2846

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.4\\(3\\)m9					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2847
Affected Version(s): 15.4\\(3\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2848

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(3\\)s0d					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2849

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.4\\(3\\)s0e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2850
Affected Version(s): 15.4\\(3\\)s0f					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2851

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.4\\(3\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2852
Affected Version(s): 15.4\\(3\\)s10					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2853

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(3\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2854

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.4\\(3\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2855
Affected Version(s): 15.4\\(3\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2856

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.4\\(3\\)s5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2857
Affected Version(s): 15.4\\(3\\)s6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2858

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(3\\)s6a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2859

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.4\\(3\\)s7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2860
Affected Version(s): 15.4\\(3\\)s8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2861

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.4\\(3\\)s9					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2862
Affected Version(s): 15.4\\(3\\)sn1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2863

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.4\\(3\\)sn1a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2864

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.5\\(1\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2865
Affected Version(s): 15.5\\(1\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2866

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.5\\(1\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2867
Affected Version(s): 15.5\\(1\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2868

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(1\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2869

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.5\\(1\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2870
Affected Version(s): 15.5\\(1\\)sn1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2871

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.5\\(1\\)sy					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2872
Affected Version(s): 15.5\\(1\\)sy1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2873

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 15.5\\(1\\)sy2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2874

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.5\\(1\\)sy3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2875
Affected Version(s): 15.5\\(1\\)sy4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2876

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.5\\(1\\)sy5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2877
Affected Version(s): 15.5\\(1\\)sy6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2878

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 15.5\\(1\\)sy7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2879

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.5\\(1\\)sy8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2880
Affected Version(s): 15.5\\(1\\)sy9					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2881

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.5\\(1\\)t					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2882
Affected Version(s): 15.5\\(1\\)t1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2883

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 15.5\\(1\\)t2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2884

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.5\\(1\\)t3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2885
Affected Version(s): 15.5\\(1\\)t4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2886

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.5\\(2\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2887
Affected Version(s): 15.5\\(2\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2888

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 15.5\\(2\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2889

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.5\\(2\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2890
Affected Version(s): 15.5\\(2\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2891

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.5\\(2\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2892
Affected Version(s): 15.5\\(2\\)t					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2893

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 15.5\\(2\\)t1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2894

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.5\\(2\\)t2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2895
Affected Version(s): 15.5\\(2\\)t3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2896

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.5\\(2\\)t4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2897
Affected Version(s): 15.5\\(2\\)xb					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2898

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 15.5\\(3\\)m					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2899

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.5\\(3\\)m0a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2900
Affected Version(s): 15.5\\(3\\)m1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2901

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.5\\(3\\)m10					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2902
Affected Version(s): 15.5\\(3\\)m11					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2903

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 15.5\\(3\\)m11a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2904

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.5\\(3\\)m2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2905
Affected Version(s): 15.5\\(3\\)m2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2906

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.5\\(3\\)m3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2907
Affected Version(s): 15.5\\(3\\)m4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2908

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(3\\)m4a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2909

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.5\\(3\\)m4b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2910
Affected Version(s): 15.5\\(3\\)m4c					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2911

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.5\\(3\\)m5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2912
Affected Version(s): 15.5\\(3\\)m6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2913

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(3\\)m6a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2914

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.5\\(3\\)m7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2915
Affected Version(s): 15.5\\(3\\)m8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2916

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.5\\(3\\)m9					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2917
Affected Version(s): 15.5\\(3\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2918

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(3\\)s0a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2919

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.5\\(3\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2920
Affected Version(s): 15.5\\(3\\)s10					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2921

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.5\\(3\\)s10a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2922
Affected Version(s): 15.5\\(3\\)s10b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2923

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(3\\)s1a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2924

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.5\\(3\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2925
Affected Version(s): 15.5\\(3\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2926

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.5\\(3\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2927
Affected Version(s): 15.5\\(3\\)s5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2928

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(3\\)s6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2929

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.5\\(3\\)s6a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2930
Affected Version(s): 15.5\\(3\\)s6b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2931

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.5\\(3\\)s7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2932
Affected Version(s): 15.5\\(3\\)s8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2933

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.5\\(3\\)s9					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2934

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.5\\(3\\)s9a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2935
Affected Version(s): 15.5\\(3\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2936

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.5\\(3\\)sn0a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2937
Affected Version(s): 15.6\\(1\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2938

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(1\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2939

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.6\\(1\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2940
Affected Version(s): 15.6\\(1\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2941

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.6\\(1\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2942
Affected Version(s): 15.6\\(1\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2943

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(1\\)sn1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2944

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.6\\(1\\)sn2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2945
Affected Version(s): 15.6\\(1\\)sn3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2946

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.6\\(1\\)t					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2947
Affected Version(s): 15.6\\(1\\)t0a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2948

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(1\\)t1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2949

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.6\\(1\\)t2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2950
Affected Version(s): 15.6\\(1\\)t3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2951

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.6\\(2\\)s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2952
Affected Version(s): 15.6\\(2\\)s1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2953

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(2\\)s2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2954

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.6\\(2\\)s3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2955
Affected Version(s): 15.6\\(2\\)s4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2956

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.6\\(2\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2957
Affected Version(s): 15.6\\(2\\)sp					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2958

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 15.6\\(2\\)sp1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2959

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.6\\(2\\)sp2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2960
Affected Version(s): 15.6\\(2\\)sp3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2961

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.6\\(2\\)sp4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2962
Affected Version(s): 15.6\\(2\\)sp5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2963

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(2\\)sp6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2964

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.6\\(2\\)sp7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2965
Affected Version(s): 15.6\\(2\\)sp8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2966

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.6\\(2\\)sp8a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2967
Affected Version(s): 15.6\\(2\\)sp9					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2968

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 15.6\\(2\\)t					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2969

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.6\\(2\\)t0a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2970
Affected Version(s): 15.6\\(2\\)t1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2971

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.6\\(2\\)t2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2972
Affected Version(s): 15.6\\(2\\)t3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2973

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 15.6\\(3\\)m					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2974

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.6\\(3\\)m0a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2975
Affected Version(s): 15.6\\(3\\)m1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2976

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.6\\(3\\)m1a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2977
Affected Version(s): 15.6\\(3\\)m1b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2978

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(3\\)m2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2979

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.6\\(3\\)m2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2980
Affected Version(s): 15.6\\(3\\)m3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/2981

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.6\\(3\\)m3a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2982
Affected Version(s): 15.6\\(3\\)m4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2983

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(3\\)m5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2984

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.6\\(3\\)m6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2985
Affected Version(s): 15.6\\(3\\)m6a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2986

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.6\\(3\\)m6b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2987
Affected Version(s): 15.6\\(3\\)m7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2988

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 15.6\\(3\\)m8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2989

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.6\\(3\\)m9					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2990
Affected Version(s): 15.6\\(3\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2991

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.6\\(4\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2992
Affected Version(s): 15.6\\(5\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2993

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.6\\(7\\)sn					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2994

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.6\\(7\\)sn1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2995
Affected Version(s): 15.6\\(7\\)sn2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2996

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.7\\(3\\)m					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2997
Affected Version(s): 15.7\\(3\\)m0a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/2998

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.7\\(3\\)m1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/2999

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.7\\(3\\)m2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3000
Affected Version(s): 15.7\\(3\\)m3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3001

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.7\\(3\\)m4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3002
Affected Version(s): 15.7\\(3\\)m4a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/3003

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.7\\(3\\)m4b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3004

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.7\\(3\\)m5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3005
Affected Version(s): 15.7\\(3\\)m6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3006

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.7\\(3\\)m7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3007
Affected Version(s): 15.7\\(3\\)m8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/3008

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 15.7\\(3\\)m9					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3009

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.8\\(3\\)m					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/3010
Affected Version(s): 15.8\\(3\\)m0a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/3011

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.8\\(3\\)m0b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3012
Affected Version(s): 15.8\\(3\\)m1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/3013

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.8\\(3\\)m1a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3014

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.8\\(3\\)m2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/3015
Affected Version(s): 15.8\\(3\\)m2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/3016

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.8\\(3\\)m3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3017
Affected Version(s): 15.8\\(3\\)m3a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/3018

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.8\\(3\\)m3b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3019

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.8\\(3\\)m4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3020
Affected Version(s): 15.8\\(3\\)m5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3021

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.8\\(3\\)m6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3022
Affected Version(s): 15.8\\(3\\)m7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/3023

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 15.8\\(3\\)m8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3024

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.9\\(3\\)m					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3025
Affected Version(s): 15.9\\(3\\)m0a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3026

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.9\\(3\\)m1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3027
Affected Version(s): 15.9\\(3\\)m2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/3028

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 15.9\\(3\\)m2a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3029

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.9\\(3\\)m3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3030
Affected Version(s): 15.9\\(3\\)m3a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3031

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 15.9\\(3\\)m3b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3032
Affected Version(s): 15.9\\(3\\)m4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS-050423/3033

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 15.9\\(3\\)m4a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS-050423/3034

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 15.9\\(3\\)m5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS-050423/3035
Affected Version(s): 17.8.1					
Out-of-bounds Write	23-Mar-2023	5.9	A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-asaftdios-dhcpv6-cli-Zf3zTv</a>	O-CIS-IOS-050423/3036

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
			<p>condition on an affected device. This vulnerability is due to insufficient validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
<b>Product: ios_xe</b>					
Affected Version(s): 17.8.1					
Out-of-bounds Write	23-Mar-2023	5.9	<p>A vulnerability in the IPv6 DHCP (DHCPv6) client module of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sasaftdios-dhcpv6-cli-Zf3zTv</a></p>	O-CIS-IOS_-050423/3037

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
			<p>validation of DHCPv6 messages. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To successfully exploit this vulnerability, the attacker would need to either control the DHCPv6 server or be in a man-in-the-middle position.</p> <p><b>CVE ID : CVE-2023-20081</b></p>		
Affected Version(s): * Up to (excluding) 16.12.8					
N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	0-CIS-IOS_-050423/3038

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 device to reload spontaneously, resulting in a DoS condition. <b>CVE ID : CVE-2023-20056</b>		
Affected Version(s): * Up to (excluding) 17.3.7					
N/A	23-Mar-2023	6.8	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-space-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-space-yejYgnNQ</a>	O-CIS-IOS_-050423/3039

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
			with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity. <b>CVE ID : CVE-2023-20082</b>		
Affected Version(s): 16.1.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3040
Affected Version(s): 16.1.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-</a>	O-CIS-IOS_-050423/3041

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
			denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	ios-dhcpv6-dos-44cMvdDK	

Affected Version(s): 16.1.3

Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3042
------------------------------------	-------------	-----	--	---	------------------------

Affected Version(s): 16.10.1

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 Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3043
Affected Version(s): 16.10.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3044

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
			exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.10.1b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3045
Affected Version(s): 16.10.1c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3046

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
			<p>vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	dos-44cMvdDK	
Affected Version(s): 16.10.1d					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3047
Affected Version(s): 16.10.1e					
Improper Validation	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6	<a href="https://sec.cloudapps.c">https://sec.cloudapps.c</a>	O-CIS-IOS_-050423/3048

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
of Array Index			(DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.10.1f					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3049

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
			device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.10.1g					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3050
Affected Version(s): 16.10.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3051

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
			data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.10.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3052
Affected Version(s): 16.10.3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	O-CIS-IOS_-050423/3053

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
			<p>IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<a href="https://content.cisco.com/content/cisco-security/cisco-sa-ios-dhcpv6-dos-44cMvdDK">ter/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	
Affected Version(s): 16.11.1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3054

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.11.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3055
Affected Version(s): 16.11.1b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3056

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.11.1c					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3057
Affected Version(s): 16.11.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3058

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.11.2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3059

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.12.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3060
Affected Version(s): 16.12.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3061

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.12.1c					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3062
Affected Version(s): 16.12.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3063

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.12.1t					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3064

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.12.1w					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3065
Affected Version(s): 16.12.1x					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3066

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.12.1y					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3067
Affected Version(s): 16.12.1z					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3068

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.12.1z1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3069

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.12.1z2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3070
Affected Version(s): 16.12.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3071

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.12.2a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3072
Affected Version(s): 16.12.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3073

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.12.2t					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3074

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.12.3					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3075
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	O-CIS-IOS_-050423/3076

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
			<p>successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Affected Version(s): 16.12.3a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3077
Affected Version(s): 16.12.3s					
Improper Validation	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6	<a href="https://sec.cloudapps.c">https://sec.cloudapps.c</a>	O-CIS-IOS_-050423/3078

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
of Array Index			(DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.12.4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	O-CIS-IOS_-050423/3079

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
			device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.12.4a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3080
Affected Version(s): 16.12.5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3081

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
			data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.12.5a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3082
Affected Version(s): 16.12.5b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3083

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
			<p>IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 16.12.6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3084

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.12.6a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3085
Affected Version(s): 16.12.7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3086

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.2.1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3087
Affected Version(s): 16.2.2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3088

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.3.1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3089

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.3.10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3090
Affected Version(s): 16.3.11					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3091

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.3.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3092
Affected Version(s): 16.3.2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3093

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.3.3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3094

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.3.4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3095
Affected Version(s): 16.3.5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3096

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.3.5b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3097
Affected Version(s): 16.3.6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3098

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 16.3.7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3099

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.3.8					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3100
Affected Version(s): 16.3.9					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3101

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.4.1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3102
Affected Version(s): 16.4.2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3103

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.4.3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3104

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.5.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3105
Affected Version(s): 16.5.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3106

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.5.1b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3107
Affected Version(s): 16.5.2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3108

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 16.5.3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3109

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.6.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3110
Affected Version(s): 16.6.10					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3111

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.6.2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3112
Affected Version(s): 16.6.3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3113

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.6.4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3114

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.6.4a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3115
Affected Version(s): 16.6.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3116

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.6.5					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3117
Affected Version(s): 16.6.5a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3118

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.6.5b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3119

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.6.6					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3120
Affected Version(s): 16.6.7					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3121

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.6.7a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3122
Affected Version(s): 16.6.8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3123

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 16.6.9					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3124

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.7.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3125
Affected Version(s): 16.7.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3126

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.7.1b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3127
Affected Version(s): 16.7.2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3128

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.7.3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3129

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.7.4					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3130
Affected Version(s): 16.8.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3131

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.8.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3132
Affected Version(s): 16.8.1b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3133

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.8.1c					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3134

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.8.1d					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3135
Affected Version(s): 16.8.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3136

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.8.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3137
Affected Version(s): 16.8.2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3138

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.8.3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3139

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.9.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3140
Affected Version(s): 16.9.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3141

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.9.1b					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3142
Affected Version(s): 16.9.1c					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3143

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.9.1d					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3144

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.9.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3145
Affected Version(s): 16.9.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3146

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.9.2a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3147
Affected Version(s): 16.9.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3148

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 16.9.3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3149

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.9.3a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3150
Affected Version(s): 16.9.3h					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3151

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.9.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3152
Affected Version(s): 16.9.4					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3153

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.9.4c					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3154

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.9.5					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3155
Affected Version(s): 16.9.5f					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3156

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 16.9.6					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3157
Affected Version(s): 16.9.7					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3158

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 16.9.8					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3159

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 16.9.8a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3160
Affected Version(s): 16.9.8b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3161

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 17.1.1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3162
Affected Version(s): 17.1.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3163

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 17.1.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3164

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 17.1.1t					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3165
Affected Version(s): 17.1.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3166

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 17.1.3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3167
Affected Version(s): 17.11.1					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3168

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
			<p>attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p> <p><b>CVE ID : CVE-2023-20065</b></p>	<p>rityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk</p>	
Affected Version(s): 17.2.1					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3169

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 17.2.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3170
Affected Version(s): 17.2.1r					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3171

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 17.2.1v					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3172
Affected Version(s): 17.2.2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3173

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 17.2.3					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3174

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 17.3.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3175
Affected Version(s): 17.3.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3176

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 17.3.1w					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3177
Affected Version(s): 17.3.1x					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3178

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 17.3.1z					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3179

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 17.3.2					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3180
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by sending a crafted request to the web UI. A	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	O-CIS-IOS_-050423/3181

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
			<p>successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Affected Version(s): 17.3.2a					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3182
Affected Version(s): 17.3.3					
Improper Validation	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6</p>	<p><a href="https://sec.cloudapps.c">https://sec.cloudapps.c</a></p>	O-CIS-IOS_-050423/3183

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
of Array Index			(DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 17.3.3a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3184

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
			device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 17.4.1					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3185
Affected Version(s): 17.4.1a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3186

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
			data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 17.4.1b					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3187
Affected Version(s): 17.4.1c					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	O-CIS-IOS_-050423/3188

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
			<p>IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 17.4.2					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3189

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 17.4.2a					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3190
Affected Version(s): 17.6.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Mar-2023	6.5	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform a directory traversal and access resources that are outside the filesystem mountpoint of the web UI. This vulnerability is due to an insufficient security configuration. An attacker could exploit this vulnerability by	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-webui-pthtrves7GSb9V</a>	O-CIS-IOS_-050423/3191

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
			<p>sending a crafted request to the web UI. A successful exploit could allow the attacker to gain read access to files that are outside the filesystem mountpoint of the web UI. Note: These files are located on a restricted filesystem that is maintained for the web UI. There is no ability to write to any files on this filesystem.</p> <p><b>CVE ID : CVE-2023-20066</b></p>		
Affected Version(s): 17.6.3					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the Cisco IOx application hosting subsystem of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to insufficient restrictions on the hosted application. An attacker could exploit this vulnerability by logging in to and then escaping the Cisco IOx application container. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-iox-priv-escalate-Xg8zkyPk</a></p>	O-CIS-IOS_-050423/3192

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
			<b>CVE ID : CVE-2023-20065</b>		
Affected Version(s): 17.7					
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	O-CIS-IOS_-050423/3193

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
			on a device to a release that would lower the attack complexity. <b>CVE ID : CVE-2023-20082</b>		
Affected Version(s): 17.9.1					
N/A	23-Mar-2023	8.6	A vulnerability in the fragmentation handling code of tunnel protocol packets in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected system to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to the improper handling of large fragmented tunnel protocol packets. One example of a tunnel protocol is Generic Routing Encapsulation (GRE). An attacker could exploit this vulnerability by sending crafted fragmented packets to an affected system. A successful exploit could allow the attacker to cause the affected system to reload, resulting in a DoS condition. Note: Only traffic directed to the affected system can be used to exploit this vulnerability. <b>CVE ID : CVE-2023-20072</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-gre-crash-p6nE5Sq5">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-gre-crash-p6nE5Sq5</a>	O-CIS-IOS_-050423/3194
Affected Version(s): 17.9.1a					
N/A	23-Mar-2023	8.6	A vulnerability in the fragmentation handling	<a href="https://sec.cloudapps.c">https://sec.cloudapps.c</a>	O-CIS-IOS_-050423/3195

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
			code of tunnel protocol packets in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected system to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to the improper handling of large fragmented tunnel protocol packets. One example of a tunnel protocol is Generic Routing Encapsulation (GRE). An attacker could exploit this vulnerability by sending crafted fragmented packets to an affected system. A successful exploit could allow the attacker to cause the affected system to reload, resulting in a DoS condition. Note: Only traffic directed to the affected system can be used to exploit this vulnerability.  <b>CVE ID : CVE-2023-20072</b>	isco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-gre-crash-p6nE5Sq5	
Affected Version(s): 17.9.1w					
N/A	23-Mar-2023	8.6	A vulnerability in the fragmentation handling code of tunnel protocol packets in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected system to reload, resulting in a denial of service (DoS) condition. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-gre-crash-p6nE5Sq5	O-CIS-IOS_-050423/3196

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
			<p>to the improper handling of large fragmented tunnel protocol packets. One example of a tunnel protocol is Generic Routing Encapsulation (GRE). An attacker could exploit this vulnerability by sending crafted fragmented packets to an affected system. A successful exploit could allow the attacker to cause the affected system to reload, resulting in a DoS condition. Note: Only traffic directed to the affected system can be used to exploit this vulnerability.</p> <p><b>CVE ID : CVE-2023-20072</b></p>		

Affected Version(s): 3.10.0ce

Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3197
------------------------------------	-------------	-----	--	--	------------------------

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
			device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.10.0e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3198
Affected Version(s): 3.10.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3199

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
			data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.10.10s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3200
Affected Version(s): 3.10.1ae					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco	<a href="https://sec.cloudapps.cisco.com/security/cen">https://sec.cloudapps.cisco.com/security/cen</a>	O-CIS-IOS_-050423/3201

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
			<p>IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>ter/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 3.10.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3202

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.10.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3203
Affected Version(s): 3.10.1se					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3204

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.10.1xbs					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3205
Affected Version(s): 3.10.1xcs					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3206

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.10.2as					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3207

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.10.2e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3208
Affected Version(s): 3.10.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3209

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.10.2ts					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3210
Affected Version(s): 3.10.3e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3211

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.10.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3212

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.10.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3213
Affected Version(s): 3.10.5s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3214

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.10.6s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3215
Affected Version(s): 3.10.7s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3216

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.10.8as					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3217

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.10.8s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3218
Affected Version(s): 3.10.9s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3219

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.11.0e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3220
Affected Version(s): 3.11.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3221

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.11.1ae					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3222

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.11.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3223
Affected Version(s): 3.11.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3224

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.11.2ae					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3225
Affected Version(s): 3.11.2e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3226

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.11.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3227

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.11.3ae					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3228
Affected Version(s): 3.11.3e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3229

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.11.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3230
Affected Version(s): 3.11.4e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3231

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.11.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3232

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.11.5e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3233
Affected Version(s): 3.11.6e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3234

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.12.0as					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3235
Affected Version(s): 3.12.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3236

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.12.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3237

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.12.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3238
Affected Version(s): 3.12.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3239

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.12.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3240
Affected Version(s): 3.13.0as					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3241

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 3.13.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3242

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.13.10s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3243
Affected Version(s): 3.13.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3244

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.13.2as					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3245
Affected Version(s): 3.13.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3246

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.13.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3247

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.13.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3248
Affected Version(s): 3.13.5as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3249

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.13.5s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3250
Affected Version(s): 3.13.6as					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3251

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.13.6bs					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3252

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.13.6s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3253
Affected Version(s): 3.13.7as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3254

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.13.7s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3255
Affected Version(s): 3.13.8s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3256

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.13.9s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3257

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.14.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3258
Affected Version(s): 3.14.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3259

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.14.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3260
Affected Version(s): 3.14.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3261

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.14.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3262

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.15.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3263
Affected Version(s): 3.15.1cs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3264

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.15.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3265
Affected Version(s): 3.15.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3266

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.15.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3267

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.15.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3268
Affected Version(s): 3.16.0as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3269

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.16.0bs					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3270
Affected Version(s): 3.16.0cs					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3271

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.16.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3272

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.16.10as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3273
Affected Version(s): 3.16.10bs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3274

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.16.10s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3275
Affected Version(s): 3.16.1as					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3276

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.16.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3277

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.16.2as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3278
Affected Version(s): 3.16.2bs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3279

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.16.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3280
Affected Version(s): 3.16.3as					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3281

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.16.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3282

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.16.4as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3283
Affected Version(s): 3.16.4bs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3284

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.16.4cs					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3285
Affected Version(s): 3.16.4ds					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3286

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.16.4es					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3287

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.16.4gs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3288
Affected Version(s): 3.16.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3289

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.16.5as					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3290
Affected Version(s): 3.16.5bs					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3291

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.16.5s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3292

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.16.6bs					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3293
Affected Version(s): 3.16.6s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3294

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.16.7as					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3295
Affected Version(s): 3.16.7bs					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3296

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 3.16.7s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3297

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.16.8s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3298
Affected Version(s): 3.16.9s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3299

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.17.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3300
Affected Version(s): 3.17.1as					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3301

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.17.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3302

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.17.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3303
Affected Version(s): 3.17.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3304

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.17.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3305
Affected Version(s): 3.18.0as					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3306

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.18.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3307

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.18.0sp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3308
Affected Version(s): 3.18.1asp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3309

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.18.1bsp					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3310
Affected Version(s): 3.18.1csp					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3311

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.18.1gsp					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3312

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.18.1hsp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3313
Affected Version(s): 3.18.1isp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3314

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.18.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3315
Affected Version(s): 3.18.1sp					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3316

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.18.2asp					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3317

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.18.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3318
Affected Version(s): 3.18.2sp					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3319

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.18.3asp					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3320
Affected Version(s): 3.18.3bsp					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3321

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.18.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3322

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.18.3sp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3323
Affected Version(s): 3.18.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3324

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.18.4sp					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3325
Affected Version(s): 3.18.5sp					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3326

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.18.6sp					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3327

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.18.7sp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3328
Affected Version(s): 3.18.8asp					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3329

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.18.8sp					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3330
Affected Version(s): 3.18.9sp					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3331

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.3.0xo					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3332

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.3.1xo					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3333
Affected Version(s): 3.3.2xo					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3334

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.4.0sg					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3335
Affected Version(s): 3.4.1sg					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3336

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 3.4.2sg					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3337

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.4.3sg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3338
Affected Version(s): 3.4.4sg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3339

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.4.5sg					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3340
Affected Version(s): 3.4.6sg					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3341

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.4.7sg					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3342

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.4.8sg					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3343
Affected Version(s): 3.5.0e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3344

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.5.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3345
Affected Version(s): 3.5.2e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3346

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.5.3e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3347

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.6.0ae					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3348
Affected Version(s): 3.6.0be					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3349

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.6.0e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3350
Affected Version(s): 3.6.10e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3351

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.6.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3352

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.6.2ae					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3353
Affected Version(s): 3.6.2e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3354

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.6.3e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3355
Affected Version(s): 3.6.4e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3356

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.6.5ae					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3357

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.6.5be					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3358
Affected Version(s): 3.6.5e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3359

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.6.6e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3360
Affected Version(s): 3.6.7ae					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3361

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.6.7be					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3362

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.6.7e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3363
Affected Version(s): 3.6.8e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3364

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.6.9ae					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3365
Affected Version(s): 3.6.9e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3366

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.7.0bs					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3367

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.7.0e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3368
Affected Version(s): 3.7.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3369

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.7.0xas					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3370
Affected Version(s): 3.7.0xbs					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3371

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.7.1as					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3372

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.7.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3373
Affected Version(s): 3.7.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3374

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.7.2e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3375
Affected Version(s): 3.7.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3376

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.7.2ts					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3377

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.7.3e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3378
Affected Version(s): 3.7.3s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3379

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.7.4as					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3380
Affected Version(s): 3.7.4e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3381

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.7.4s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3382

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.7.5e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3383
Affected Version(s): 3.7.5s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3384

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.7.6s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3385
Affected Version(s): 3.7.7s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3386

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 3.7.8s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3387

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.8.0e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3388
Affected Version(s): 3.8.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3389

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.8.10ce					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3390
Affected Version(s): 3.8.10e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3391

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor y/cisco-sa- ios-dhcpv6- dos- 44cMvdDK	
Affected Version(s): 3.8.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/y/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3392

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.8.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3393
Affected Version(s): 3.8.2e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3394

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.8.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3395
Affected Version(s): 3.8.3e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3396

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p>rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</p>	
Affected Version(s): 3.8.4e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3397

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.8.5ae					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3398
Affected Version(s): 3.8.5e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3399

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.8.6e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3400
Affected Version(s): 3.8.7e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3401

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.8.8e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3402

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.8.9e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3403
Affected Version(s): 3.9.0as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3404

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.9.0e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3405
Affected Version(s): 3.9.0s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3406

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.9.0xas					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3407

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.9.1as					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3408
Affected Version(s): 3.9.1e					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3409

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
			<p>this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>		
Affected Version(s): 3.9.1s					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3410
Affected Version(s): 3.9.2be					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecu</a></p>	O-CIS-IOS_-050423/3411

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
			<p>unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p> <p><b>CVE ID : CVE-2023-20080</b></p>	rityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK	
Affected Version(s): 3.9.2e					
Improper Validation of Array Index	23-Mar-2023	7.5	<p>A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a></p>	O-CIS-IOS_-050423/3412

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
			<b>CVE ID : CVE-2023-20080</b>		
Affected Version(s): 3.9.2s					
Improper Validation of Array Index	23-Mar-2023	7.5	A vulnerability in the IPv6 DHCP version 6 (DHCPv6) relay and server features of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to trigger a denial of service (DoS) condition. This vulnerability is due to insufficient validation of data boundaries. An attacker could exploit this vulnerability by sending crafted DHCPv6 messages to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly.  <b>CVE ID : CVE-2023-20080</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-dhcpv6-dos-44cMvdDK</a>	O-CIS-IOS_-050423/3413
Affected Version(s): From (including) 17.1 Up to (excluding) 17.3.6					
N/A	23-Mar-2023	5.5	A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	O-CIS-IOS_-050423/3414

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
			<p>vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>		
Affected Version(s): From (including) 17.4 Up to (excluding) 17.6.5					
N/A	23-Mar-2023	6.8	<p>A vulnerability in Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches could allow an authenticated, local attacker with level-15 privileges or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to errors that occur when retrieving the public release key that is used for image signature verification. An attacker could exploit this vulnerability by modifying specific variables in the Serial Peripheral Interface (SPI) flash memory of an affected device. A successful exploit could allow the attacker to execute persistent code on the underlying</p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-c9300-spi-ace-yejYgnNQ</a></p>	O-CIS-IOS_-050423/3415

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
			<p>operating system. Note: In Cisco IOS XE Software releases 16.11.1 and later, the complexity of an attack using this vulnerability is high. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software on a device to a release that would lower the attack complexity.</p> <p><b>CVE ID : CVE-2023-20082</b></p>		
N/A	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<p><a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a></p>	O-CIS-IOS_-050423/3416
Affected Version(s): From (including) 17.7 Up to (excluding) 17.9.2					

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	23-Mar-2023	5.5	<p>A vulnerability in the management CLI of Cisco access point (AP) software could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to cause an affected device to reload spontaneously, resulting in a DoS condition.</p> <p><b>CVE ID : CVE-2023-20056</b></p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ap-cli-dos-tc2EKEpu</a>	O-CIS-IOS_-050423/3417
<b>Product: ios_xe_sd-wan</b>					
Affected Version(s): -					
N/A	23-Mar-2023	7.8	<p>A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with elevated privileges. This vulnerability is due to insufficient input validation by the system CLI. An attacker with privileges to run commands could exploit this vulnerability by first authenticating to an</p>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-ios-xe-sdwan-VQAhEjYw</a>	O-CIS-IOS_-050423/3418

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
			<p>affected device using either local terminal access or a management shell interface and then submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system. Note: For additional information about specific impacts, see the Details section of this advisory.</p> <p><b>CVE ID : CVE-2023-20035</b></p>		
<b>Vendor: contiki-ng</b>					
<b>Product: contiki-ng</b>					
Affected Version(s): * Up to (including) 4.8					
Out-of-bounds Write	17-Mar-2023	9.8	<p>Contiki-NG is an open-source, cross-platform operating system for internet of things (IoT) devices. In versions 4.8 and prior, an out-of-bounds write can occur in the BLE L2CAP module of the Contiki-NG operating system. The network stack of Contiki-NG uses a global buffer (packetbuf) for processing of packets, with the size of PACKETBUF_SIZE. In</p>	<p><a href="https://github.com/contiki-ng/contiki-ng/pull/2398">https://github.com/contiki-ng/contiki-ng/pull/2398</a>,  <a href="https://github.com/contiki-ng/security/advisories/GHSA-m737-4vx6-pfq">https://github.com/contiki-ng/security/advisories/GHSA-m737-4vx6-pfq</a></p>	O-CON-CONT-050423/3419

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
			<p>particular, when using the BLE L2CAP module with the default configuration, the PACKETBUF_SIZE value becomes larger than the actual size of the packetbuf. When large packets are processed by the L2CAP module, a buffer overflow can therefore occur when copying the packet data to the packetbuf. The vulnerability has been patched in the "develop" branch of Contiki-NG, and will be included in release 4.9. The problem can be worked around by applying the patch manually.</p> <p><b>CVE ID : CVE-2023-28116</b></p>		

**Vendor: Debian**

**Product: debian\_linux**

Affected Version(s): 10.0

<p>Authorization Bypass Through User-Controlled Key</p>	<p>24-Mar-2023</p>	<p>7.1</p>	<p>Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information.</p> <p><b>CVE ID : CVE-2023-28686</b></p>	<p><a href="https://dino.im/security/cve-2023-28686/">https://dino.im/security/cve-2023-28686/</a></p>	<p>O-DEB-DEBI-050423/3420</p>
---	--------------------	------------	---	--	-------------------------------

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): 11.0					
Authorization Bypass Through User-Controlled Key	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information.  <b>CVE ID : CVE-2023-28686</b>	<a href="https://dino.im/security/cve-2023-28686/">https://dino.im/security/cve-2023-28686/</a>	O-DEB-DEBI-050423/3421
Affected Version(s): 12.0					
Authorization Bypass Through User-Controlled Key	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information.  <b>CVE ID : CVE-2023-28686</b>	<a href="https://dino.im/security/cve-2023-28686/">https://dino.im/security/cve-2023-28686/</a>	O-DEB-DEBI-050423/3422
<b>Vendor: dek-1705_project</b>					
<b>Product: dek-1705_firmware</b>					
Affected Version(s): 34.23.1					
Improper Neutralization of Special Elements used in a	24-Mar-2023	9.8	DEK-1705 <=Firmware:34.23.1 device was discovered to have a command execution vulnerability.	N/A	O-DEK-DEK--050423/3423

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			<b>CVE ID : CVE-2023-23149</b>		
<b>Vendor: Dell</b>					
<b>Product: embedded_box_pc_3000_firmware</b>					
Affected Version(s): * Up to (excluding) 1.18.0					
Improper Input Validation	16-Mar-2023	6.7	Dell BIOS contains an Improper Input Validation vulnerability. A local authenticated malicious user with administrator privileges could potentially exploit this vulnerability to perform arbitrary code execution.  <b>CVE ID : CVE-2023-24571</b>	<a href="https://www.dell.com/support/kbdoc/en-us/000210955/dsa-2023-046">https://www.dell.com/support/kbdoc/en-us/000210955/dsa-2023-046</a>	O-DEL-EMBE-050423/3424
<b>Vendor: Dlink</b>					
<b>Product: dir820la1_firmware</b>					
Affected Version(s): 105b03					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Mar-2023	9.8	OS Command injection vulnerability in D-Link DIR820LA1_FW105B03 allows attackers to escalate privileges to root via a crafted payload with the ping_addr parameter to ping.ccp.  <b>CVE ID : CVE-2023-25280</b>	<a href="https://www.dlink.com/en/security-bulletin/">https://www.dlink.com/en/security-bulletin/</a>	O-DLI-DIR8-050423/3425
Out-of-bounds Write	16-Mar-2023	7.5	A stack overflow vulnerability exists in pingV4Msg component in D-Link DIR820LA1_FW105B03, allows attackers to cause a denial of service via the	<a href="https://www.dlink.com/en/security-bulletin/">https://www.dlink.com/en/security-bulletin/</a>	O-DLI-DIR8-050423/3426

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
			nextPage parameter to ping.ccp. <b>CVE ID : CVE-2023-25281</b>		
<b>Vendor: Fedoraproject</b>					
<b>Product: fedora</b>					
Affected Version(s): 36					
Improper Control of Generation of Code ('Code Injection')	23-Mar-2023	9.8	The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS). <b>CVE ID : CVE-2023-28333</b>	<a href="https://moodle.org/mod/forum/discuss.php?d=445065">https://moodle.org/mod/forum/discuss.php?d=445065</a>	O-FED-FEDO-050423/3427
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/003320.html">https://lists.x.org/archives/xorg-announce/2023-February/003320.html</a>	O-FED-FEDO-050423/3428
Authorization Bypass Through User-	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store	<a href="https://dino.im/security/cve-2023-28686/">https://dino.im/security/cve-2023-28686/</a>	O-FED-FEDO-050423/3429

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
Controlled Key			<p>via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information.</p> <p><b>CVE ID : CVE-2023-28686</b></p>		
Improper Input Validation	23-Mar-2023	5.5	<p>A vulnerability was discovered in ImageMagick where a specially created SVG file loads itself and causes a segmentation fault. This flaw allows a remote attacker to pass a specially crafted SVG file that leads to a segmentation fault, generating many trash files in "/tmp," resulting in a denial of service. When ImageMagick crashes, it generates a lot of trash files. These trash files can be large if the SVG file contains many render actions. In a denial of service attack, if a remote attacker uploads an SVG file of size t, ImageMagick generates files of size 103*t. If an attacker uploads a 100M SVG, the server will generate about 10G.</p> <p><b>CVE ID : CVE-2023-1289</b></p>	<p><a href="https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4">https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4</a>,  <a href="https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr">https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr</a>,  <a href="https://bugzilla.redhat.com/show_bug.cgi?id=2176858">https://bugzilla.redhat.com/show_bug.cgi?id=2176858</a></p>	O-FED-FEDO-050423/3430
Affected Version(s): 37					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/03320.html">https://lists.x.org/archives/xorg-announce/2023-February/03320.html</a>	O-FED-FEDO-050423/3431
Authorization Bypass Through User-Controlled Key	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change the display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information. <b>CVE ID : CVE-2023-28686</b>	<a href="https://dino.im/security/cve-2023-28686/">https://dino.im/security/cve-2023-28686/</a>	O-FED-FEDO-050423/3432
Improper Input Validation	23-Mar-2023	5.5	A vulnerability was discovered in ImageMagick where a specially created SVG file loads itself and causes a segmentation fault. This flaw allows a remote attacker to pass a specially crafted SVG file that leads to a	<a href="https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4">https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4</a> ,	O-FED-FEDO-050423/3433

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
			segmentation fault, generating many trash files in "/tmp," resulting in a denial of service. When ImageMagick crashes, it generates a lot of trash files. These trash files can be large if the SVG file contains many render actions. In a denial of service attack, if a remote attacker uploads an SVG file of size t, ImageMagick generates files of size 103*t. If an attacker uploads a 100M SVG, the server will generate about 10G. <b>CVE ID : CVE-2023-1289</b>	<a href="https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr">https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr</a> , <a href="https://bugzilla.redhat.com/show_bug.cgi?id=2176858">https://bugzilla.redhat.com/show_bug.cgi?id=2176858</a>	
Allocation of Resources Without Limits or Throttling	23-Mar-2023	5.5	A flaw was found in the QEMU implementation of VMWare's paravirtual RDMA device. This flaw allows a crafted guest driver to allocate and initialize a huge number of page tables to be used as a ring of descriptors for CQ and async events, potentially leading to an out-of-bounds read and crash of QEMU. <b>CVE ID : CVE-2023-1544</b>	<a href="https://lists.nongnu.org/archive/html/qemu-devel/2023-03/msg00206.html">https://lists.nongnu.org/archive/html/qemu-devel/2023-03/msg00206.html</a> , <a href="https://bugzilla.redhat.com/show_bug.cgi?id=2180364">https://bugzilla.redhat.com/show_bug.cgi?id=2180364</a>	O-FED-FEDO-050423/3434
Affected Version(s): 38					
Authorization Bypass Through User-Controlled Key	24-Mar-2023	7.1	Dino before 0.2.3, 0.3.x before 0.3.2, and 0.4.x before 0.4.2 allows attackers to modify the personal bookmark store via a crafted message. The attacker can change	<a href="https://dino.im/security/cve-2023-28686/">https://dino.im/security/cve-2023-28686/</a>	O-FED-FEDO-050423/3435

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 display of group chats or force a victim to join a group chat; the victim may then be tricked into disclosing sensitive information. <b>CVE ID : CVE-2023-28686</b>		
<b>Vendor: Google</b>					
<b>Product: android</b>					
Affected Version(s): -					
Out-of-bounds Write	24-Mar-2023	9.8	In ProfSixDecomTcpSACKop tion of RohcPacketCommon, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244450646References: N/A <b>CVE ID : CVE-2023-21057</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3436
Out-of-bounds Write	24-Mar-2023	9.8	In lcs_m_SendRrAcquiAssist of lcs_m_bcm_assist.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3437

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
			for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 246169606References: N/A <b>CVE ID : CVE-2023- 21058</b>		
N/A	24-Mar- 2023	7.8	In buildCommand of bluetooth_ccc.cc, there is a possible out of bounds write due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 238420277References: N/A <b>CVE ID : CVE-2023- 21040</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR- 050423/3438
Out-of- bounds Write	24-Mar- 2023	7.8	In append_to_params of param_util.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 250123688References: N/A	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR- 050423/3439

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
			<b>CVE ID : CVE-2023-21041</b>		
N/A	24-Mar-2023	7.8	In (TBD) of (TBD), there is a possible way to boot with a hidden debug policy due to a missing warning to the user. This could lead to local escalation of privilege after preparing the device, hiding the warning, and passing the phone to a new user, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243433344References: N/A <b>CVE ID : CVE-2023-21068</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3440
Out-of-bounds Read	24-Mar-2023	7.5	In sms_GetTpPile of sms_PduCodec.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-253770924References: N/A	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3441

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
			<b>CVE ID : CVE-2023-21060</b>		
Out-of-bounds Read	24-Mar-2023	7.5	In EUTRAN_LCS_DecodeFacilityInformationElement of LPP_LcsManagement.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-247564044References: N/A <b>CVE ID : CVE-2023-21059</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3442
Out-of-bounds Read	24-Mar-2023	7.5	In sms_ExtractCbLanguage of sms_CellBroadcast.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-251805610References: N/A	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3443

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
			<b>CVE ID : CVE-2023-21053</b>		
N/A	24-Mar-2023	7.5	Product: AndroidVersions: Android kernelAndroid ID: A-254114726References: N/A <b>CVE ID : CVE-2023-21067</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3444
N/A	24-Mar-2023	7.5	Product: AndroidVersions: Android kernelAndroid ID: A-229255400References: N/A <b>CVE ID : CVE-2023-21061</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3445
Out-of-bounds Write	24-Mar-2023	7.2	In EUTRAN_LCS_ConvertLCS_MOLRRReq of LPP_CommonUtil.c, there is a possible out of bounds write due to a logic error in the code. This could lead to remote code execution with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244556535References: N/A <b>CVE ID : CVE-2023-21054</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3446
Out-of-bounds Write	24-Mar-2023	6.7	In cs40l2x_cp_trigger_queue_show of cs40l2x.c, there is a possible out of	<a href="https://source.android.com/security/bulletin">https://source.android.com/security/bulletin</a>	O-GOO-ANDR-050423/3447

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
			bounds write due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-224000736References: N/A <b>CVE ID : CVE-2023-21038</b>	/pixel/2023-03-01	
Out-of-bounds Write	24-Mar-2023	6.7	In rtt_unpack_xtlv_cbfn of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257289560References: N/A <b>CVE ID : CVE-2023-21077</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3448
Use After Free	24-Mar-2023	6.7	In (TBD) of (TBD), there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product:	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3449

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
			<p>AndroidVersions:            Android kernelAndroid            ID: A-            239873326References:            N/A</p> <p><b>CVE ID : CVE-2023-            21042</b></p>		
Use After Free	24-Mar-2023	6.7	<p>In (TBD) of (TBD), there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product:            AndroidVersions:            Android kernelAndroid            ID: A-            239872581References:            N/A</p> <p><b>CVE ID : CVE-2023-            21043</b></p>	<p><a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a></p>	0-GOO-ANDR-050423/3450
Out-of-bounds Write	24-Mar-2023	6.7	<p>In rtt_unpack_xtlv_cbf of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product:            AndroidVersions:            Android kernelAndroid            ID: A-            254840211References:            N/A</p> <p><b>CVE ID : CVE-2023-            21078</b></p>	<p><a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a></p>	0-GOO-ANDR-050423/3451

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-Mar-2023	6.7	In load_png_image of ExynosHWCHelper.cpp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244423702References: N/A <b>CVE ID : CVE-2023-21050</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3452
Out-of-bounds Write	24-Mar-2023	6.7	In dwc3_exynos_clk_get of dwc3-exynos.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-259323322References: N/A <b>CVE ID : CVE-2023-21051</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3453
Out-of-bounds Write	24-Mar-2023	6.7	In setToExternal of ril_external_client.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local	<a href="https://source.android.com/security/bulletin">https://source.android.com/security/bulletin</a>	O-GOO-ANDR-050423/3454

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
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-259063189References: N/A <b>CVE ID : CVE-2023-21052</b>	/pixel/2023-03-01	
Access of Resource Using Incompatible Type ('Type Confusion')	24-Mar-2023	6.7	In lwis_slc_buffer_free of lwis_device_slc.c, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-245300559References: N/A <b>CVE ID : CVE-2023-21056</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3455
Out-of-bounds Write	24-Mar-2023	6.7	In rtt_unpack_xtlv_cbf of dhd_rtt.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3456

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
			ID: A-254839721References: N/A <b>CVE ID : CVE-2023-21079</b>		
Out-of-bounds Read	24-Mar-2023	6.7	In DoSetTempEcc of imsservice.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243376770References: N/A <b>CVE ID : CVE-2023-21062</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3457
Out-of-bounds Read	24-Mar-2023	6.7	In ParseWithAuthType of simdata.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243129862References: N/A <b>CVE ID : CVE-2023-21063</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3458

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	24-Mar-2023	6.7	In DoSetPinControl of miscservice.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243130078References: N/A <b>CVE ID : CVE-2023-21064</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3459
Integer Overflow or Wraparound	24-Mar-2023	6.7	In fdt_next_tag of fdt.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239630493References: N/A <b>CVE ID : CVE-2023-21065</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3460
Out-of-bounds Write	24-Mar-2023	6.7	In wl_update_hidden_ap_ie of wl_cfgscan.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3461

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
			<p>execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254029309References: N/A</p> <p><b>CVE ID : CVE-2023-21069</b></p>		
Out-of-bounds Write	24-Mar-2023	6.7	<p>In add_roam_cache_list of wl_roam.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-254028776References: N/A</p> <p><b>CVE ID : CVE-2023-21070</b></p>	<p><a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a></p>	O-GOO-ANDR-050423/3462
Out-of-bounds Write	24-Mar-2023	6.7	<p>In dhd_prot_ioctcmplt_process of dhd_msgbuf.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:</p>	<p><a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a></p>	O-GOO-ANDR-050423/3463

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
			Android kernelAndroid ID: A-254028518References: N/A <b>CVE ID : CVE-2023-21071</b>		
Out-of-bounds Write	24-Mar-2023	6.7	In rtt_unpack_xtlv_cbf of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257290781References: N/A <b>CVE ID : CVE-2023-21072</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3464
Out-of-bounds Write	24-Mar-2023	6.7	In rtt_unpack_xtlv_cbf of dhd_rtt.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-257290396References: N/A <b>CVE ID : CVE-2023-21073</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3465

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-Mar-2023	6.7	In get_svc_hash of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857862References: N/A <b>CVE ID : CVE-2023-21075</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3466
Out-of-bounds Write	24-Mar-2023	6.7	In createTransmitFollowup Request of nan.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-261857623References: N/A <b>CVE ID : CVE-2023-21076</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3467
Use After Free	24-Mar-2023	6.4	In dit_hal_ioctl of dit.c, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System	<a href="https://source.android.com/security/bulletin">https://source.android.com/security/bulletin</a>	O-GOO-ANDR-050423/3468

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
			<p>execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244301523References: N/A</p> <p><b>CVE ID : CVE-2023-21055</b></p>	/pixel/2023-03-01	
N/A	24-Mar-2023	5.5	<p>In BitmapExport.java, there is a possible failure to truncate images due to a logic error in the code.Product: AndroidVersions: Android kernelAndroid ID: A-264261868References: N/A</p> <p><b>CVE ID : CVE-2023-21036</b></p>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3469
Out-of-bounds Read	24-Mar-2023	4.4	<p>In dumpstateBoard of Dumpstate.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-263783650References: N/A</p> <p><b>CVE ID : CVE-2023-21039</b></p>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3470

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 Restriction of Operations within the Bounds of a Memory Buffer	24-Mar-2023	4.4	In init of VendorGraphicBufferMeta, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-253425086References: N/A <b>CVE ID : CVE-2023-21044</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3471
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-Mar-2023	4.4	In ConvertToHalMetadata of aidl_utils.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-256166866References: N/A <b>CVE ID : CVE-2023-21047</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3472
Out-of-bounds Write	24-Mar-2023	4.4	In ConvertToHalMetadata of aidl_utils.cc, there is a possible out of bounds read due to an incorrect bounds check. This could	<a href="https://source.android.com/security/bulletin">https://source.android.com/security/bulletin</a>	O-GOO-ANDR-050423/3473

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
			lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-253424924References: N/A <b>CVE ID : CVE-2023-21046</b>	/pixel/2023-03-01	
Use After Free	24-Mar-2023	4.4	When cpif handles probe failures, there is a possible out of bounds read due to a use after free. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-259323725References: N/A <b>CVE ID : CVE-2023-21045</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3474
Out-of-bounds Read	24-Mar-2023	4.4	In append_camera_metadata of camera_metadata.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product:	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3475

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
			<p>AndroidVersions: Android kernelAndroid ID: A- 236688120References: N/A</p> <p><b>CVE ID : CVE-2023- 21049</b></p>		
Out-of-bounds Read	24-Mar-2023	4.4	<p>In handleEvent of nan.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A- 259304053References: N/A</p> <p><b>CVE ID : CVE-2023- 21048</b></p>	<p><a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a></p>	O-GOO-ANDR-050423/3476
Affected Version(s): 11.0					
Out-of-bounds Write	24-Mar-2023	9.8	<p>In gatt_process_prep_write_rsp of gatt_cl.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-</p>	<p><a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a></p>	O-GOO-ANDR-050423/3477

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
			13Android ID: A-258652631 <b>CVE ID : CVE-2023-20951</b>		
Out-of-bounds Write	24-Mar-2023	9.8	In SDP_AddAttribute of sdp_db.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261867748 <b>CVE ID : CVE-2023-20954</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3478
N/A	24-Mar-2023	7.8	In onPackageAddedInternal of PermissionManagerService.java, there is a possible way to silently grant a permission after a Target SDK update due to a permissions bypass. This could lead to local escalation of privilege after updating an app to a higher Target SDK with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3479

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
			13Android ID: A-221040577 <b>CVE ID : CVE-2023-20906</b>		
Uncontrolled Resource Consumption	24-Mar-2023	7.8	In addPermission of PermissionManagerServiceImpl.java , there is a possible failure to persist permission settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242537498 <b>CVE ID : CVE-2023-20911</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3480
N/A	24-Mar-2023	7.8	In onTargetSelected of ResolverActivity.java, there is a possible way to share a wrong file due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242605257	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3481

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
			<b>CVE ID : CVE-2023-20917</b>		
Out-of-bounds Write	24-Mar-2023	7.8	In avdt_scb_hdl_write_req of avdt_scb_act.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242535997 <b>CVE ID : CVE-2023-20931</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3482
Out-of-bounds Write	24-Mar-2023	7.8	In bta_av_rc_disc_done of bta_av_act.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-226927612 <b>CVE ID : CVE-2023-20936</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3483
Missing Authorization	24-Mar-2023	7.8	In onPrepareOptionsMenu of	<a href="https://source.android.com/secu">https://source.android.com/secu</a>	O-GOO-ANDR-050423/3484

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
			AppInfoDashboardFragment.java, there is a possible way to bypass admin restrictions and uninstall applications for all users due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-258653813 <b>CVE ID : CVE-2023-20955</b>	ity/bulletin/2023-03-01	
N/A	24-Mar-2023	7.8	In onAttach of SettingsPreferenceFragment.java, there is a possible bypass of Factory Reset Protections due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-258422561 <b>CVE ID : CVE-2023-20957</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3485

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 Certificate Validation	24-Mar-2023	7.8	In WorkSource, there is a possible parcel mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-220302519 <b>CVE ID : CVE-2023-20963</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3486
Out-of-bounds Write	24-Mar-2023	7.8	In inflate of inflate.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242299736 <b>CVE ID : CVE-2023-20966</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3487
Uncontrolled Resource Consumption	24-Mar-2023	5.5	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3488

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
			additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920 <b>CVE ID : CVE-2023-20910</b>		
Out-of-bounds Write	24-Mar-2023	5.5	In A2DP_BuildCodecHeader Sbc of a2dp_sbc.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-186803518 <b>CVE ID : CVE-2023-20952</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3489
N/A	16-Mar-2023	3.3	Improper access control vulnerability in MyFiles application prior to versions 12.2.09.0 in Android 11, 13.1.03.501 in Android 12 and 14.1.03.0 in Android 13 allows local attacker to get sensitive information of secret mode in Samsung Internet	<a href="https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03">https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03</a>	O-GOO-ANDR-050423/3490

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
			application with specific conditions. <b>CVE ID : CVE-2023-21463</b>		
Affected Version(s): 12.0					
Out-of-bounds Write	24-Mar-2023	9.8	In gatt_process_prep_write_rsp of gatt_cl.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-258652631 <b>CVE ID : CVE-2023-20951</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3491
Out-of-bounds Write	24-Mar-2023	9.8	In SDP_AddAttribute of sdp_db.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261867748 <b>CVE ID : CVE-2023-20954</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3492

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	24-Mar-2023	7.8	In onPackageAddedInternal of PermissionManagerService.java, there is a possible way to silently grant a permission after a Target SDK update due to a permissions bypass. This could lead to local escalation of privilege after updating an app to a higher Target SDK with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-221040577 <b>CVE ID : CVE-2023-20906</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3493
Uncontrolled Resource Consumption	24-Mar-2023	7.8	In addPermission of PermissionManagerServiceImpl.java , there is a possible failure to persist permission settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242537498	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3494

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
			<b>CVE ID : CVE-2023-20911</b>		
N/A	24-Mar-2023	7.8	In onTargetSelected of ResolverActivity.java, there is a possible way to share a wrong file due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242605257 <b>CVE ID : CVE-2023-20917</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3495
Out-of-bounds Write	24-Mar-2023	7.8	In avdt_scb_hdl_write_req of avdt_scb_act.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242535997 <b>CVE ID : CVE-2023-20931</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3496

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-Mar-2023	7.8	In bta_av_rc_disc_done of bta_av_act.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-226927612 <b>CVE ID : CVE-2023-20936</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3497
N/A	24-Mar-2023	7.8	In getGroupState of GrantPermissionsViewModel.kt, there is a possible way to keep a one-time permission granted due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-237405974 <b>CVE ID : CVE-2023-20947</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3498
Missing Authorization	24-Mar-2023	7.8	In onPrepareOptionsMenu of AppInfoDashboardFragment.java, there is a possible way to bypass	<a href="https://source.android.com/security/bulletin">https://source.android.com/security/bulletin</a>	O-GOO-ANDR-050423/3499

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
			admin restrictions and uninstall applications for all users due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-258653813 <b>CVE ID : CVE-2023-20955</b>	/2023-03-01	
N/A	24-Mar-2023	7.8	In onAttach of SettingsPreferenceFragment.java, there is a possible bypass of Factory Reset Protections due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-258422561 <b>CVE ID : CVE-2023-20957</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3500
Improper Certificate Validation	24-Mar-2023	7.8	In WorkSource, there is a possible parcel mismatch. This could lead to local escalation of privilege with no additional execution privileges	<a href="https://source.android.com/security/bulletin">https://source.android.com/security/bulletin</a>	O-GOO-ANDR-050423/3501

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
			needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-220302519 <b>CVE ID : CVE-2023-20963</b>	/2023-03-01	
N/A	24-Mar-2023	7.8	In multiple functions of MediaSessionRecord.java , there is a possible Intent rebroadcast due to a confused deputy. This could lead to local denial of service or escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-238177121 <b>CVE ID : CVE-2023-20964</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3502
Out-of-bounds Write	24-Mar-2023	7.8	In inflate of inflate.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3503

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
			13Android ID: A-242299736 <b>CVE ID : CVE-2023-20966</b>		
Missing Authorization	24-Mar-2023	6.8	In onParentVisible of HeaderPrivacyIconsController.kt, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-253043058 <b>CVE ID : CVE-2023-20926</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3504
Uncontrolled Resource Consumption	24-Mar-2023	5.5	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3505

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
			13Android ID: A-245299920 <b>CVE ID : CVE-2023-20910</b>		
Out-of-bounds Write	24-Mar-2023	5.5	In A2DP_BuildCodecHeader Sbc of a2dp_sbc.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-186803518 <b>CVE ID : CVE-2023-20952</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3506
Out-of-bounds Write	24-Mar-2023	4.4	In Import of C2SurfaceSyncObj.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-240140929 <b>CVE ID : CVE-2023-20956</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3507

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-Mar-2023	3.3	The sensitive information exposure vulnerability in Quick Share Agent prior to versions 3.5.14.18 in Android 12 and 3.5.16.20 in Android 13 allows to local attacker to access MAC address without related permission. <b>CVE ID : CVE-2023-21462</b>	<a href="https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03">https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03</a>	O-GOO-ANDR-050423/3508
N/A	16-Mar-2023	3.3	Improper access control vulnerability in MyFiles application prior to versions 12.2.09.0 in Android 11, 13.1.03.501 in Android 12 and 14.1.03.0 in Android 13 allows local attacker to get sensitive information of secret mode in Samsung Internet application with specific conditions. <b>CVE ID : CVE-2023-21463</b>	<a href="https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03">https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03</a>	O-GOO-ANDR-050423/3509
N/A	16-Mar-2023	3.3	Improper access control in Samsung Calendar prior to versions 12.4.02.9000 in Android 13 and 12.3.08.2000 in Android 12 allows local attacker to configure improper status. <b>CVE ID : CVE-2023-21464</b>	<a href="https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03">https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03</a>	O-GOO-ANDR-050423/3510
Affected Version(s): 12.1					
Out-of-bounds Write	24-Mar-2023	9.8	In gatt_process_prep_write_rsp of gatt_cl.cc, there is a possible out of bounds write due to a missing	<a href="https://source.android.com/security/bulletin">https://source.android.com/security/bulletin</a>	O-GOO-ANDR-050423/3511

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
			bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-258652631 <b>CVE ID : CVE-2023-20951</b>	/2023-03-01	
Out-of-bounds Write	24-Mar-2023	9.8	In SDP_AddAttribute of sdp_db.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261867748 <b>CVE ID : CVE-2023-20954</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3512
Improper Input Validation	24-Mar-2023	8.8	In launchDeepLinkIntentToRight of SettingsHomepageActivity.java, there is a possible way to launch arbitrary activities due to improper input validation. This could lead to local escalation of privilege with User	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3513

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
			<p>execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12L Android-13Android ID: A-250589026</p> <p><b>CVE ID : CVE-2023-20960</b></p>		
N/A	24-Mar-2023	7.8	<p>In onPackageAddedInternal of PermissionManagerService.java, there is a possible way to silently grant a permission after a Target SDK update due to a permissions bypass. This could lead to local escalation of privilege after updating an app to a higher Target SDK with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-221040577</p> <p><b>CVE ID : CVE-2023-20906</b></p>	<p><a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a></p>	O-GOO-ANDR-050423/3514
Uncontrolled Resource Consumption	24-Mar-2023	7.8	<p>In addPermission of PermissionManagerServiceImpl.java , there is a possible failure to persist permission settings due to resource exhaustion. This could lead to local escalation of privilege with no additional</p>	<p><a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a></p>	O-GOO-ANDR-050423/3515

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
			<p>execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242537498</p> <p><b>CVE ID : CVE-2023-20911</b></p>		
N/A	24-Mar-2023	7.8	<p>In onTargetSelected of ResolverActivity.java, there is a possible way to share a wrong file due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242605257</p> <p><b>CVE ID : CVE-2023-20917</b></p>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3516
Out-of-bounds Write	24-Mar-2023	7.8	<p>In avdt_scb_hdl_write_req of avdt_scb_act.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:</p>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3517

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
			Android-11 Android-12 Android-12L Android- 13Android ID: A- 242535997 <b>CVE ID : CVE-2023- 20931</b>		
Out-of- bounds Write	24-Mar- 2023	7.8	In bta_av_rc_disc_done of bta_av_act.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A- 226927612 <b>CVE ID : CVE-2023- 20936</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR- 050423/3518
N/A	24-Mar- 2023	7.8	In getGroupState of GrantPermissionsViewM odel.kt, there is a possible way to keep a one-time permission granted due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-237405974	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR- 050423/3519

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
			<b>CVE ID : CVE-2023-20947</b>		
Missing Authorization	24-Mar-2023	7.8	In onPrepareOptionsMenu of AppInfoDashboardFragment.java, there is a possible way to bypass admin restrictions and uninstall applications for all users due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-258653813 <b>CVE ID : CVE-2023-20955</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3520
N/A	24-Mar-2023	7.8	In onAttach of SettingsPreferenceFragment.java, there is a possible bypass of Factory Reset Protections due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-258422561	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3521

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
			<b>CVE ID : CVE-2023-20957</b>		
Improper Certificate Validation	24-Mar-2023	7.8	In WorkSource, there is a possible parcel mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-220302519 <b>CVE ID : CVE-2023-20963</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3522
N/A	24-Mar-2023	7.8	In multiple functions of MediaSessionRecord.java , there is a possible Intent rebroadcast due to a confused deputy. This could lead to local denial of service or escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-238177121 <b>CVE ID : CVE-2023-20964</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3523
Out-of-bounds Write	24-Mar-2023	7.8	In inflate of inflate.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3524

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
			with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242299736 <b>CVE ID : CVE-2023-20966</b>		
Missing Authorization	24-Mar-2023	6.8	In onParentVisible of HeaderPrivacyIconsController.kt, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-253043058 <b>CVE ID : CVE-2023-20926</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3525
Uncontrolled Resource Consumption	24-Mar-2023	5.5	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3526

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
			additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245299920 <b>CVE ID : CVE-2023-20910</b>		
Out-of-bounds Write	24-Mar-2023	5.5	In A2DP_BuildCodecHeader Sbc of a2dp_sbc.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-186803518 <b>CVE ID : CVE-2023-20952</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3527
Out-of-bounds Write	24-Mar-2023	4.4	In Import of C2SurfaceSyncObj.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3528

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
			Android-12 Android-12L Android-13Android ID: A-240140929  <b>CVE ID : CVE-2023-20956</b>		
Affected Version(s): 13.0					
Out-of-bounds Write	24-Mar-2023	9.8	In gatt_process_prep_write_rsp of gatt_cl.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-258652631  <b>CVE ID : CVE-2023-20951</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3529
Out-of-bounds Write	24-Mar-2023	9.8	In SDP_AddAttribute of sdp_db.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261867748	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3530

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
			<b>CVE ID : CVE-2023-20954</b>		
Improper Input Validation	24-Mar-2023	8.8	In launchDeepLinkIntentTo Right of SettingsHomepageActivity.java, there is a possible way to launch arbitrary activities due to improper input validation. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12L Android-13Android ID: A-250589026 <b>CVE ID : CVE-2023-20960</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3531
Missing Authorization	24-Mar-2023	7.8	In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261193711 <b>CVE ID : CVE-2023-21003</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3532

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
Uncontrolled Resource Consumption	24-Mar-2023	7.8	In addPermission of PermissionManagerServiceImpl.java , there is a possible failure to persist permission settings due to resource exhaustion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242537498 <b>CVE ID : CVE-2023-20911</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3533
N/A	24-Mar-2023	7.8	In onTargetSelected of ResolverActivity.java, there is a possible way to share a wrong file due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242605257 <b>CVE ID : CVE-2023-20917</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3534
N/A	24-Mar-2023	7.8	In InstallStart of InstallStart.java, there is a possible way to change the installer package	<a href="https://source.android.com/security/bulletin">https://source.android.com/security/bulletin</a>	O-GOO-ANDR-050423/3535

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			name due to an improper input validation. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-236687884 <b>CVE ID : CVE-2023-21017</b>	/pixel/2023-03-01	
Missing Authorization	24-Mar-2023	7.8	In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-244569778 <b>CVE ID : CVE-2023-21015</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3536
Out-of-bounds Write	24-Mar-2023	7.8	In avdt_scb_hdl_write_req of avdt_scb_act.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3537

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
			<p>AndroidVersions:            Android-11 Android-12            Android-12L Android-            13Android ID: A-            242535997</p> <p><b>CVE ID : CVE-2023-            20931</b></p>		
Out-of-bounds Write	24-Mar-2023	7.8	<p>In bta_av_rc_disc_done of bta_av_act.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-226927612</p> <p><b>CVE ID : CVE-2023-            20936</b></p>	<p><a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a></p>	O-GOO-ANDR-050423/3538
N/A	24-Mar-2023	7.8	<p>In getGroupState of GrantPermissionsViewModel.kt, there is a possible way to keep a one-time permission granted due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-237405974</p>	<p><a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a></p>	O-GOO-ANDR-050423/3539

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
			<b>CVE ID : CVE-2023-20947</b>		
Missing Authorization	24-Mar-2023	7.8	In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261193946 <b>CVE ID : CVE-2023-21005</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3540
N/A	24-Mar-2023	7.8	In onPrimaryClipChanged of ClipboardListener.java, there is a possible way to bypass factory reset protection due to incorrect UI being shown prior to setup completion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-251778420 <b>CVE ID : CVE-2023-20953</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3541

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	24-Mar-2023	7.8	In onPrepareOptionsMenu of AppInfoDashboardFragment.java, there is a possible way to bypass admin restrictions and uninstall applications for all users due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-258653813 <b>CVE ID : CVE-2023-20955</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3542
Out-of-bounds Write	24-Mar-2023	7.8	In BTA_GATTS_HandleValue Indication of bta_gatts_api.cc, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-245915315 <b>CVE ID : CVE-2023-20985</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3543

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	24-Mar-2023	7.8	In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261193664 <b>CVE ID : CVE-2023-21004</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3544
Missing Authorization	24-Mar-2023	7.8	In AddSupervisedUserActivity, guest users are not prevented from starting the activity due to missing permissions checks. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-249057848 <b>CVE ID : CVE-2023-20959</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3545
N/A	24-Mar-2023	7.8	In onPackageAddedInternal of PermissionManagerService.java, there is a possible way to silently grant a permission after a Target	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3546

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
			<p>SDK update due to a permissions bypass. This could lead to local escalation of privilege after updating an app to a higher Target SDK with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-221040577</p> <p><b>CVE ID : CVE-2023-20906</b></p>		
Missing Authorization	24-Mar-2023	7.8	<p>In getAvailabilityStatus of several Transcode Permission Controllers, there is a possible permission bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261193935</p> <p><b>CVE ID : CVE-2023-21002</b></p>	<p><a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a></p>	O-GOO-ANDR-050423/3547
Improper Certificate Validation	24-Mar-2023	7.8	<p>In WorkSource, there is a possible parcel mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for</p>	<p><a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a></p>	O-GOO-ANDR-050423/3548

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
			<p>exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A- 220302519</p> <p><b>CVE ID : CVE-2023- 20963</b></p>		
N/A	24-Mar-2023	7.8	<p>In multiple functions of MediaSessionRecord.java , there is a possible Intent rebroadcast due to a confused deputy. This could lead to local denial of service or escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-238177121</p> <p><b>CVE ID : CVE-2023- 20964</b></p>	<p><a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a></p>	O-GOO-ANDR-050423/3549
Out-of-bounds Write	24-Mar-2023	7.8	<p>In inflate of inflate.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A- 242299736</p>	<p><a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a></p>	O-GOO-ANDR-050423/3550

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
			<b>CVE ID : CVE-2023-20966</b>		
Missing Authorization	24-Mar-2023	7.8	In onContextItemSelected of NetworkProviderSettings.java, there is a possible way for users to change the Wi-Fi settings of other users due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-237672190 <b>CVE ID : CVE-2023-21001</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3551
Improper Locking	24-Mar-2023	7.8	In MediaCodec.cpp, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-194783918 <b>CVE ID : CVE-2023-21000</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3552
N/A	24-Mar-2023	7.8	In captureImage of CustomizedSensor.cpp, there is a possible way to bypass the fingerprint unlock due to a logic	<a href="https://source.android.com/security/bulletin">https://source.android.com/security/bulletin</a>	O-GOO-ANDR-050423/3553

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
			error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-241910279 <b>CVE ID : CVE-2023-20995</b>	/pixel/2023-03-01	
N/A	24-Mar-2023	7.8	In updatePermissionTreeSourcePackage of PermissionManagerServiceImpl.java, there is a possible way to obtain dangerous permission without the user's consent due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-225880325 <b>CVE ID : CVE-2023-20971</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3554
Improper Handling of Exceptional Conditions	24-Mar-2023	7.8	In multiple functions of SnoozeHelper.java, there is a possible failure to persist settings due to an uncaught exception. This could lead to local escalation of privilege with no additional	N/A	O-GOO-ANDR-050423/3555

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
			<p>execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-261588851</p> <p><b>CVE ID : CVE-2023-20993</b></p>		
Incorrect Authorization	24-Mar-2023	7.8	<p>In multiple functions of BackupHelper.java, there is a possible way for an app to get permissions previously granted to another app with the same package name due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-184847040</p> <p><b>CVE ID : CVE-2023-21035</b></p>	<p><a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a></p>	O-GOO-ANDR-050423/3556
Incorrect Authorization	24-Mar-2023	7.8	<p>In multiple functions of SensorService.cpp, there is a possible access of accurate sensor data due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:</p>	<p><a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a></p>	O-GOO-ANDR-050423/3557

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
			Android-13Android ID: A-230358834 <b>CVE ID : CVE-2023-21034</b>		
N/A	24-Mar-2023	7.8	In getAvailabilityStatus of EnableContentCapturePreferenceController.java, there is a possible way to bypass DISALLOW_CONTENT_CAPTURE due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-250573776 <b>CVE ID : CVE-2023-20975</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3558
Double Free	24-Mar-2023	7.8	In Confirmation of keystore_cli_v2.cpp, there is a possible way to corrupt memory due to a double free. This could lead to local escalation of privilege in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-226234140 <b>CVE ID : CVE-2023-21030</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3559

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	24-Mar-2023	7.8	In maybeFinish of FallbackHome.java, there is a possible delay of lockdown screen due to logic error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246543238 <b>CVE ID : CVE-2023-21024</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3560
Out-of-bounds Write	24-Mar-2023	7.8	In BufferBlock of Suballocation.cpp, there is a possible out of bounds write due to memory corruption. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-236098131 <b>CVE ID : CVE-2023-21022</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3561
Missing Authorization	24-Mar-2023	7.8	In isTargetSdkLessThanQOrPrivileged of WifiServiceImpl.java, there is a possible way for the guest user to change admin user network settings due to a missing permission check. This could lead to	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3562

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
			local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-255537598 <b>CVE ID : CVE-2023-21021</b>		
Out-of-bounds Read	24-Mar-2023	7.5	In parse_printerAttributes of ipphelper.c, there is a possible out of bounds read due to a string without a null-terminator. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-180680572 <b>CVE ID : CVE-2023-21028</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3563
N/A	24-Mar-2023	7.5	In serializePasspointConfiguration of PasspointXmlUtils.java, there is a possible logic error in the code. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3564

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
			<p>AndroidVersions: Android-13Android ID: A-216854451</p> <p><b>CVE ID : CVE-2023-21027</b></p>		
Improper Input Validation	24-Mar-2023	7.3	<p>In getConfirmationMessage of DefaultAutofillPicker.java , there is a possible way to mislead the user to select default autofill application due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-216117246</p> <p><b>CVE ID : CVE-2023-20976</b></p>	<p><a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a></p>	O-GOO-ANDR-050423/3565
Out-of-bounds Read	24-Mar-2023	7.1	<p>In read_paint of ttcolr.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-254803162</p> <p><b>CVE ID : CVE-2023-20958</b></p>	<p><a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a></p>	O-GOO-ANDR-050423/3566

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	24-Mar-2023	6.8	In onParentVisible of HeaderPrivacyIconsController.kt, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-253043058 <b>CVE ID : CVE-2023-20926</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3567
Out-of-bounds Write	24-Mar-2023	6.7	In _ufdt_output_property_to_fdt of ufdt_convert.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-259062118 <b>CVE ID : CVE-2023-20994</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3568
Use After Free	24-Mar-2023	6.7	In UnwindingWorker of unwinding.cc, there is a possible out of bounds write due to a use after	<a href="https://source.android.com/security/bulletin">https://source.android.com/security/bulletin</a>	O-GOO-ANDR-050423/3569

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
			free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-233338564 <b>CVE ID : CVE-2023-21018</b>	/pixel/2023-03-01	
Use After Free	24-Mar-2023	6.7	In registerSignalHandlers of main.c, there is a possible local arbitrary code execution due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-256591441 <b>CVE ID : CVE-2023-21020</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3570
Uncontrolled Resource Consumption	24-Mar-2023	5.5	In addNetworkSuggestions of WifiManager.java, there is a possible way to trigger permanent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3571

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
			Android-12L Android-13Android ID: A-245299920 <b>CVE ID : CVE-2023-20910</b>		
N/A	24-Mar-2023	5.5	In sendHalfSheetCancelBroadcast of HalfSheetActivity.java, there is a possible way to learn nearby BT MAC addresses due to an unrestricted broadcast intent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-234442700 <b>CVE ID : CVE-2023-20929</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3572
Out-of-bounds Write	24-Mar-2023	5.5	In A2DP_BuildCodecHeaderSbc of a2dp_sbc.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3573

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
			13Android ID: A-186803518 <b>CVE ID : CVE-2023-20952</b>		
Loop with Unreachable Exit Condition ('Infinite Loop')	24-Mar-2023	5.5	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749936 <b>CVE ID : CVE-2023-20998</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3574
N/A	24-Mar-2023	5.5	In getSliceEndItem of MediaVolumePreferenceController.java, there is a possible way to start foreground activity from the background due to an unsafe PendingIntent. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-256590210 <b>CVE ID : CVE-2023-20962</b>	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3575
Loop with Unreachable	24-Mar-2023	5.5	In multiple locations, there is a possible way to	<a href="https://source.android">https://source.android</a>	O-GOO-ANDR-050423/3576

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
e Exit Condition ('Infinite Loop')			trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246750467 <b>CVE ID : CVE-2023-20999</b>	.com/security/bulletin/pixel/2023-03-01	
N/A	24-Mar-2023	5.5	In AccountTypePreference of AccountTypePreference.java, there is a possible way to mislead the user about accounts installed on the device due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-213905884 <b>CVE ID : CVE-2023-21016</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3577
Improper Restriction of Operations within the Bounds of	24-Mar-2023	5.5	In btm_vendor_specific_evt of btm_devctl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3578

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
a Memory Buffer			disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-255304665 <b>CVE ID : CVE-2023-20972</b>		
Loop with Unreachable Exit Condition ('Infinite Loop')	24-Mar-2023	5.5	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749764 <b>CVE ID : CVE-2023-20996</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3579
Loop with Unreachable Exit Condition ('Infinite Loop')	24-Mar-2023	5.5	In multiple locations, there is a possible way to trigger a persistent reboot loop due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246749702	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3580

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
			<b>CVE ID : CVE-2023-20997</b>		
Out-of-bounds Read	24-Mar-2023	5.5	In ih264e_init_proc_ctxt of ih264e_process.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-242379731 <b>CVE ID : CVE-2023-21019</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3581
Out-of-bounds Read	24-Mar-2023	5.5	In btu_ble_ll_conn_param_upd_evt of btu_hcif.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260230274 <b>CVE ID : CVE-2023-20980</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3582
Out-of-bounds Read	24-Mar-2023	5.5	In BtaAvCo::GetNextSourceDataPacket of bta_av_co.cc, there is a possible out of bounds	<a href="https://source.android.com/security/bulletin">https://source.android.com/security/bulletin</a>	O-GOO-ANDR-050423/3583

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
			read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-259939364 <b>CVE ID : CVE-2023-20979</b>	/pixel/2023-03-01	
N/A	24-Mar-2023	5.5	In updateInputChannel of WindowManagerService.java, there is a possible way to set a touchable region beyond its own SurfaceControl due to a logic error in the code. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-254681548 <b>CVE ID : CVE-2023-21026</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3584
Missing Authorization	24-Mar-2023	5.5	In register of UidObserverController.java, there is a missing permission check. This could lead to local information disclosure of app usage with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3585

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
			Android-13Android ID: A-217934898 <b>CVE ID : CVE-2023-21029</b>		
Uncontrolled Resource Consumption	24-Mar-2023	5.5	In addNetwork of WifiManager.java, there is a possible way to trigger a persistent DoS due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-244713323 <b>CVE ID : CVE-2023-21033</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3586
Out-of-bounds Read	24-Mar-2023	5.5	In btm_ble_add_resolving_list_entry_complete of btm_ble_privacy.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260078907 <b>CVE ID : CVE-2023-20974</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3587
Out-of-bounds Read	24-Mar-2023	5.5	In btm_create_conn_cancel_complete of btm_sec.cc,	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3588

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
			there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568245 <b>CVE ID : CVE-2023-20973</b>	ity/bulletin/pixel/2023-03-01	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	24-Mar-2023	4.7	In Display::setPowerMode of HWC2.cpp, there is a possible out of bounds read due to a race condition. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-242688355 <b>CVE ID : CVE-2023-21031</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3589
Out-of-bounds Read	24-Mar-2023	4.5	In btm_read_rssi_complete of btm_acl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3590

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
			for exploitation.Product: AndroidVersions: Android-13Android ID: A-260569232 <b>CVE ID : CVE-2023-20988</b>		
Out-of-bounds Read	24-Mar-2023	4.5	In btm_read_link_quality_complete of btm_acl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure over Bluetooth with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260569414 <b>CVE ID : CVE-2023-20987</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3591
Out-of-bounds Read	24-Mar-2023	4.5	In on_iso_link_quality_read of btm_iso_impl.h, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568750 <b>CVE ID : CVE-2023-20992</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3592

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029912 <b>CVE ID : CVE-2023-21011</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3593
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029812 <b>CVE ID : CVE-2023-21012</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3594
Out-of-bounds Read	24-Mar-2023	4.4	In forceStaDisconnection of hostapd.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product:	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3595

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
			AndroidVersions: Android-13Android ID: A-256818945 <b>CVE ID : CVE-2023-21013</b>		
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029326 <b>CVE ID : CVE-2023-21014</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3596
Out-of-bounds Read	24-Mar-2023	4.4	In btm_ble_rand_enc_complete of btm_sec.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260569449 <b>CVE ID : CVE-2023-20983</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3597
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing	<a href="https://source.android.com/security/bulletin">https://source.android.com/security/bulletin</a>	O-GOO-ANDR-050423/3598

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
			bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029915 <b>CVE ID : CVE-2023-21010</b>	/pixel/2023-03-01	
Out-of-bounds Read	24-Mar-2023	4.4	In btm_read_tx_power_complete of btm_acl.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the Bluetooth server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568083 <b>CVE ID : CVE-2023-20982</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3599
Out-of-bounds Write	24-Mar-2023	4.4	In Import of C2SurfaceSyncObj.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L	<a href="https://source.android.com/security/bulletin/2023-03-01">https://source.android.com/security/bulletin/2023-03-01</a>	O-GOO-ANDR-050423/3600

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
			Android-13Android ID: A-240140929 <b>CVE ID : CVE-2023-20956</b>		
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262235935 <b>CVE ID : CVE-2023-20968</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3601
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262236313 <b>CVE ID : CVE-2023-20969</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3602
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3603

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
			disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262236005 <b>CVE ID : CVE-2023-20970</b>		
Out-of-bounds Read	24-Mar-2023	4.4	In btm_read_local_oob_complete of btm_sec.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568354 <b>CVE ID : CVE-2023-20990</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3604
Out-of-bounds Read	24-Mar-2023	4.4	In btm_ble_read_remote_features_complete of btm_ble_gap.cc, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure if the firmware were compromised with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3605

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
			Android-13Android ID: A-254445952 <b>CVE ID : CVE-2023-20977</b>		
Out-of-bounds Read	24-Mar-2023	4.4	In ufdt_local_fixup_prop of ufdt_overlay.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-254929746 <b>CVE ID : CVE-2023-21025</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3606
Out-of-bounds Read	24-Mar-2023	4.4	In btm_ble_write_adv_enable_complete of btm_ble_gap.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-260568367 <b>CVE ID : CVE-2023-20989</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3607
Out-of-bounds Read	24-Mar-2023	4.4	In btu_ble_rc_param_req_evt of btu_hcif.cc, there is a possible out of bounds	<a href="https://source.android.com/security/bulletin">https://source.android.com/security/bulletin</a>	O-GOO-ANDR-050423/3608

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
			read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-256165737 <b>CVE ID : CVE-2023-20981</b>	/pixel/2023-03-01	
Out-of-bounds Read	24-Mar-2023	4.4	In btm_ble_process_periodic_adv_sync_lost_evt of ble_scanner_hci_interface.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-255305114 <b>CVE ID : CVE-2023-20991</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3609
Out-of-bounds Read	24-Mar-2023	4.4	In ParseBqrLinkQualityEvt of btif_bqr.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product:	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3610

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
			AndroidVersions: Android-13Android ID: A-242993878 <b>CVE ID : CVE-2023-20984</b>		
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257030027 <b>CVE ID : CVE-2023-21006</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3611
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029965 <b>CVE ID : CVE-2023-21007</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3612
Out-of-bounds Read	24-Mar-2023	4.4	In _ufdt_output_node_to_fdt of ufdt_convert.c, there is a possible out of bounds read due to a heap buffer	<a href="https://source.android.com/security/bulletin">https://source.android.com/security/bulletin</a>	O-GOO-ANDR-050423/3613

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
			overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-248085351 <b>CVE ID : CVE-2023-21032</b>	/pixel/2023-03-01	
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257030100 <b>CVE ID : CVE-2023-21008</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3614
Out-of-bounds Read	24-Mar-2023	4.4	In multiple locations of p2p_iface.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-257029925	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3615

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
			<b>CVE ID : CVE-2023-21009</b>		
Out-of-bounds Read	24-Mar-2023	4.4	In btm_ble_clear_resolving_list_complete of btm_ble_privacy.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-255304475 <b>CVE ID : CVE-2023-20986</b>	<a href="https://source.android.com/security/bulletin/pixel/2023-03-01">https://source.android.com/security/bulletin/pixel/2023-03-01</a>	O-GOO-ANDR-050423/3616
N/A	16-Mar-2023	3.3	The sensitive information exposure vulnerability in Quick Share Agent prior to versions 3.5.14.18 in Android 12 and 3.5.16.20 in Android 13 allows to local attacker to access MAC address without related permission. <b>CVE ID : CVE-2023-21462</b>	<a href="https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03">https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03</a>	O-GOO-ANDR-050423/3617
N/A	16-Mar-2023	3.3	Improper access control vulnerability in MyFiles application prior to versions 12.2.09.0 in Android 11, 13.1.03.501 in Android 12 and 14.1.03.0 in Android 13 allows local attacker to get sensitive information of secret mode in Samsung Internet	<a href="https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03">https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03</a>	O-GOO-ANDR-050423/3618

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
			application with specific conditions. <b>CVE ID : CVE-2023-21463</b>		
N/A	16-Mar-2023	3.3	Improper access control in Samsung Calendar prior to versions 12.4.02.9000 in Android 13 and 12.3.08.2000 in Android 12 allows local attacker to configure improper status. <b>CVE ID : CVE-2023-21464</b>	<a href="https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03">https://security.samsungmobile.com/serviceWeb.smsb?year=2023&amp;month=03</a>	O-GOO-ANDR-050423/3619
<b>Vendor: hgiga</b>					
<b>Product: powerstation_firmware</b>					
Affected Version(s): * Up to (excluding) x64.6.2.165					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27-Mar-2023	8.8	HGiga PowerStation remote management function has insufficient filtering for user input. An authenticated remote attacker with general user privilege can exploit this vulnerability to inject and execute arbitrary system commands to perform arbitrary system operation or disrupt service. <b>CVE ID : CVE-2023-24837</b>	<a href="https://www.twcert.org.tw/tw/cp-132-6956-fbd85-1.html">https://www.twcert.org.tw/tw/cp-132-6956-fbd85-1.html</a>	O-HGI-POWE-050423/3620
Missing Authentication for Critical Function	27-Mar-2023	7.5	HGiga PowerStation has a vulnerability of Information Leakage. An unauthenticated remote attacker can exploit this vulnerability to obtain the administrator's credential, resulting in performing arbitrary	<a href="https://www.twcert.org.tw/tw/cp-132-6957-d8f67-1.html">https://www.twcert.org.tw/tw/cp-132-6957-d8f67-1.html</a>	O-HGI-POWE-050423/3621

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
			system operation or disrupt service. <b>CVE ID : CVE-2023-24838</b>		
<b>Vendor: HP</b>					
<b>Product: integrated_lights-out_4</b>					
Affected Version(s): * Up to (excluding) 2.82					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	O-HP-INTE-050423/3622
<b>Product: integrated_lights-out_5</b>					
Affected Version(s): * Up to (excluding) 2.78					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out. <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	O-HP-INTE-050423/3623
<b>Product: integrated_lights-out_6</b>					
Affected Version(s): * Up to (excluding) 1.20					

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')	22-Mar-2023	5.4	A remote Cross-site Scripting vulnerability was discovered in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE has provided software updates to resolve this vulnerability in HPE Integrated Lights-Out.  <b>CVE ID : CVE-2023-28083</b>	<a href="https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us">https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&amp;docId=hpesbhf04456en_us</a>	O-HP-INTE-050423/3624
<b>Vendor: hpe</b>					
<b>Product: arubaos-cx</b>					
Affected Version(s): From (including) 10.06.0000 Up to (excluding) 10.06.0240					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX.  <b>CVE ID : CVE-2023-1168</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	O-HPE-ARUB-050423/3625
Affected Version(s): From (including) 10.08.0000 Up to (including) 10.08.1070					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	O-HPE-ARUB-050423/3626

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
			in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>		
Affected Version(s): From (including) 10.09.0000 Up to (including) 10.09.1020					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX. <b>CVE ID : CVE-2023-1168</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	O-HPE-ARUB-050423/3627
Affected Version(s): From (including) 10.10.0000 Up to (excluding) 10.10.1030					
N/A	22-Mar-2023	8.8	An authenticated remote code execution vulnerability exists in the AOS-CX Network Analytics Engine. Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system, leading to a complete compromise of the switch running AOS-CX.	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-004.txt</a>	O-HPE-ARUB-050423/3628

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
			<b>CVE ID : CVE-2023-1168</b>		
<b>Vendor: jcgcn.com</b>					
<b>Product: jhr-n916r_firmware</b>					
Affected Version(s): * Up to (including) 21.11.1.1483					
N/A	16-Mar-2023	9.8	Command execution vulnerability was discovered in JHR-N916R router firmware version<=21.11.1.1483. <b>CVE ID : CVE-2023-24795</b>	N/A	O-JCG-JHR--050423/3629
<b>Vendor: lancombg</b>					
<b>Product: sa-wr915nd_firmware</b>					
Affected Version(s): 17.35.1					
N/A	16-Mar-2023	9.8	SA-WR915ND router firmware v17.35.1 was discovered to be vulnerable to code execution. <b>CVE ID : CVE-2023-23150</b>	N/A	O-LAN-SA-W-050423/3630
<b>Vendor: Linux</b>					
<b>Product: linux_kernel</b>					
Affected Version(s): -					
N/A	22-Mar-2023	8.8	TXOne StellarOne has an improper access control privilege escalation vulnerability in every version before V2.0.1160 that could allow a malicious, falsely authenticated user to escalate his privileges to administrator level. With these privileges, an attacker could perform actions they are not authorized to. Please note: an attacker must	<a href="https://success.trendmicro.com/solution/000292486">https://success.trendmicro.com/solution/000292486</a>	O-LIN-LINU-050423/3631

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
			first obtain a low-privileged authenticated user's profile on the target system in order to exploit this vulnerability. <b>CVE ID : CVE-2023-25069</b>		
Improper Restriction of XML External Entity Reference	21-Mar-2023	8.8	IBM Aspera Faspex 4.4.2 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote authenticated attacker could exploit this vulnerability to execute arbitrary commands. IBM X-Force ID: 249845. <b>CVE ID : CVE-2023-27874</b>	<a href="https://www.ibm.com/support/pages/node/6964694">https://www.ibm.com/support/pages/node/6964694</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/249845">https://exchange.xforce.ibmcloud.com/vulnerabilities/249845</a>	O-LIN-LINU-050423/3632
Improper Privilege Management	22-Mar-2023	7.8	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious users to execute arbitrary code with root level privileges on the Linux instance. <b>CVE ID : CVE-2023-25590</b>	<a href="https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt">https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-003.txt</a>	O-LIN-LINU-050423/3633
Improper Neutralization of Special Elements used in an SQL Command	21-Mar-2023	7.5	IBM Aspera Faspex 4.4.2 could allow a remote attacker to obtain sensitive credential information for an external user, using a specially crafted SQL	<a href="https://www.ibm.com/support/pages/node/6964694">https://www.ibm.com/support/pages/node/6964694</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/249845">https://exchange.xforce.ibmcloud.com/vulnerabilities/249845</a>	O-LIN-LINU-050423/3634

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			query. IBM X-Force ID: 249613. <b>CVE ID : CVE-2023-27871</b>	com/vulnerabilities/249613	
N/A	16-Mar-2023	7.5	IBM Aspera Faspex 5.0.4 could allow a user to change other user's credentials due to improper access controls. IBM X-Force ID: 249847. <b>CVE ID : CVE-2023-27875</b>	<a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/249847">https://exchange.xforce.ibmcloud.com/vulnerabilities/249847</a> , <a href="https://www.ibm.com/support/pages/node/6963662">https://www.ibm.com/support/pages/node/6963662</a>	O-LIN-LINU-050423/3635
N/A	21-Mar-2023	6.5	IBM Aspera Faspex 4.4.2 could allow a remote authenticated attacker to obtain sensitive credential information using specially crafted XML input. IBM X-Force ID: 249654. <b>CVE ID : CVE-2023-27873</b>	<a href="https://www.ibm.com/support/pages/node/6964694">https://www.ibm.com/support/pages/node/6964694</a> , <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/249654">https://exchange.xforce.ibmcloud.com/vulnerabilities/249654</a>	O-LIN-LINU-050423/3636
Affected Version(s): * Up to (excluding) 5.11					
N/A	16-Mar-2023	7.5	A remote denial of service vulnerability was found in the Linux kernel's TIPC kernel module. The while loop in tipc_link_xmit() hits an unknown state while attempting to parse SKBs, which are not in the queue. Sending two small UDP packets to a system with a UDP bearer results in the CPU utilization for the system to instantly spike to 100%, causing a	<a href="https://github.com/torvalds/linux/commit/b77413446408fdd256599daf00d5be72b5f3e7c6">https://github.com/torvalds/linux/commit/b77413446408fdd256599daf00d5be72b5f3e7c6</a> , <a href="https://infosec.exchange/@_matata/109427999461122360">https://infosec.exchange/@_matata/109427999461122360</a>	O-LIN-LINU-050423/3637

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
			denial of service condition. <b>CVE ID : CVE-2023-1390</b>		
Affected Version(s): * Up to (excluding) 5.13.3					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Mar-2023	7.8	An issue was discovered in the Linux kernel before 5.13.3. lib/seq_buf.c has a seq_buf_putmem_hex buffer overflow. <b>CVE ID : CVE-2023-28772</b>	<a href="https://github.com/torvalds/linux/commit/d3b16034a24a112bb83aeb669ac5b9b01f744bb7">https://github.com/torvalds/linux/commit/d3b16034a24a112bb83aeb669ac5b9b01f744bb7</a> , <a href="https://lkml.kernel.org/r/20210626032156.47889-1-yun.zhou@windriver.com">https://lkml.kernel.org/r/20210626032156.47889-1-yun.zhou@windriver.com</a> , <a href="https://lore.kernel.org/lkml/20210625122453.5e2fe304@oasis.local.home/">https://lore.kernel.org/lkml/20210625122453.5e2fe304@oasis.local.home/</a>	O-LIN-LINU-050423/3638
Affected Version(s): * Up to (excluding) 5.16					
Use After Free	23-Mar-2023	7.8	A use-after-free flaw was found in the Linux kernel's Ext4 File System in how a user triggers several file operations simultaneously with the overlay FS usage. This flaw allows a local user to crash or potentially escalate their privileges on the system. Only if patch 9a2544037600 ("ovl: fix use after free in	<a href="https://lore.kernel.org/lkml/20211115165433.449951285@linuxfoundation.org/">https://lore.kernel.org/lkml/20211115165433.449951285@linuxfoundation.org/</a>	O-LIN-LINU-050423/3639

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
			struct ovl_aio_req") not applied yet, the kernel could be affected. <b>CVE ID : CVE-2023-1252</b>		
Affected Version(s): * Up to (excluding) 5.18					
Use After Free	23-Mar-2023	5.5	A use-after-free flaw was found in the Linux kernel's core dump subsystem. This flaw allows a local user to crash the system. Only if patch 390031c94211 ("coredump: Use the vma snapshot in fill_files_note") not applied yet, then kernel could be affected. <b>CVE ID : CVE-2023-1249</b>	<a href="https://patchwork.kernel.org/project/linux-fsdevel/patch/87iltzn3nd.fsf_-_@email.forward.int.ebiederm.org/">https://patchwork.kernel.org/project/linux-fsdevel/patch/87iltzn3nd.fsf_-_@email.forward.int.ebiederm.org/</a>	O-LIN-LINU-050423/3640
Affected Version(s): * Up to (excluding) 6.1					
Use After Free	23-Mar-2023	4.7	A use-after-free flaw was found in qdisc_graft in net/sched/sch_api.c in the Linux Kernel due to a race problem. This flaw leads to a denial of service issue. If patch ebda44da44f6 ("net: sched: fix race condition in qdisc_graft()") not applied yet, then kernel could be affected. <b>CVE ID : CVE-2023-0590</b>	<a href="https://lore.kernel.org/all/20221018203258.2793282-1-edumazet@google.com/">https://lore.kernel.org/all/20221018203258.2793282-1-edumazet@google.com/</a>	O-LIN-LINU-050423/3641
Affected Version(s): * Up to (excluding) 6.2					
N/A	22-Mar-2023	7.8	A flaw was found in the Linux kernel, where unauthorized access to the execution of the setuid file with capabilities was found in the Linux kernel's OverlayFS subsystem in	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?i">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?i</a>	O-LIN-LINU-050423/3642

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
			how a user copies a capable file from a nosuid mount into another mount. This uid mapping bug allows a local user to escalate their privileges on the system. <b>CVE ID : CVE-2023-0386</b>	d=4f11ada 10d0a	
Affected Version(s): * Up to (excluding) 6.3					
Use After Free	27-Mar-2023	6.8	A flaw was found in the Linux kernel. A use-after-free may be triggered in asus_kbd_backlight_set when plugging/disconnecting in a malicious USB device, which advertises itself as an Asus device. Similarly to the previous known CVE-2023-25012, but in asus devices, the work_struct may be scheduled by the LED controller while the device is disconnecting, triggering a use-after-free on the struct asus_kbd_leds *led structure. A malicious USB device may exploit the issue to cause memory corruption with controlled data. <b>CVE ID : CVE-2023-1079</b>	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/next/linux-next.git/commit/?id=4ab3a086d10eeec1424f2e8a968827a6336203df">https://git.kernel.org/pub/scm/linux/kernel/git/next/linux-next.git/commit/?id=4ab3a086d10eeec1424f2e8a968827a6336203df</a>	O-LIN-LINU-050423/3643
Affected Version(s): * Up to (including) 6.2.6					
NULL Pointer Dereference	16-Mar-2023	7	do_tls_getsockopt in net/tls/tls_main.c in the Linux kernel through 6.2.6 lacks a lock_sock call, leading to a race condition (with a resultant use-after-free	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id</a>	O-LIN-LINU-050423/3644

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
			or NULL pointer dereference). <b>CVE ID : CVE-2023-28466</b>	=49c47cc2 1b5b7a3d8 deb18fc57 b0aa2ab12 86962	
Affected Version(s): 5.11					
N/A	16-Mar-2023	7.5	A remote denial of service vulnerability was found in the Linux kernel's TIPC kernel module. The while loop in tipc_link_xmit() hits an unknown state while attempting to parse SKBs, which are not in the queue. Sending two small UDP packets to a system with a UDP bearer results in the CPU utilization for the system to instantly spike to 100%, causing a denial of service condition. <b>CVE ID : CVE-2023-1390</b>	<a href="https://github.com/torvalds/linux/commit/b77413446408fdd256599daf00d5be72b5f3e7c6">https://github.com/torvalds/linux/commit/b77413446408fdd256599daf00d5be72b5f3e7c6</a> , <a href="https://infosec.exchange/@matata/109427999461122360">https://infosec.exchange/@matata/109427999461122360</a>	O-LIN-LINU-050423/3645
Affected Version(s): 5.19					
NULL Pointer Dereference	24-Mar-2023	5.5	A NULL pointer dereference was found in io_file_bitmap_get in io_uring/filetable.c in the io_uring sub-component in the Linux Kernel. When fixed files are unregistered, some context information (file_alloc_{start,end} and alloc_hint) is not cleared. A subsequent request that has auto index selection enabled via IORING_FILE_INDEX_ALL OC can cause a NULL pointer dereference. An	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/axboe/linux-block.git/commit/?h=io_uring-6.3&amp;id=761efd55a0227aca3a69deacdaa112fffd44fe37">https://git.kernel.org/pub/scm/linux/kernel/git/axboe/linux-block.git/commit/?h=io_uring-6.3&amp;id=761efd55a0227aca3a69deacdaa112fffd44fe37</a>	O-LIN-LINU-050423/3646

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
			unprivileged user can use the flaw to cause a system crash. <b>CVE ID : CVE-2023-1583</b>		
Affected Version(s): 6.0					
NULL Pointer Dereference	24-Mar-2023	5.5	A NULL pointer dereference was found in io_file_bitmap_get in io_uring/filetable.c in the io_uring sub-component in the Linux Kernel. When fixed files are unregistered, some context information (file_alloc_{start,end} and alloc_hint) is not cleared. A subsequent request that has auto index selection enabled via IORING_FILE_INDEX_ALL OC can cause a NULL pointer dereference. An unprivileged user can use the flaw to cause a system crash. <b>CVE ID : CVE-2023-1583</b>	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/axboe/linux-block.git/commit/?h=io_uring-6.3&amp;id=761efd55a0227aca3a69deacdaa112fffd44fe37">https://git.kernel.org/pub/scm/linux/kernel/git/axboe/linux-block.git/commit/?h=io_uring-6.3&amp;id=761efd55a0227aca3a69deacdaa112fffd44fe37</a>	O-LIN-LINU-050423/3647
Affected Version(s): 6.1					
NULL Pointer Dereference	24-Mar-2023	5.5	A NULL pointer dereference was found in io_file_bitmap_get in io_uring/filetable.c in the io_uring sub-component in the Linux Kernel. When fixed files are unregistered, some context information (file_alloc_{start,end} and alloc_hint) is not cleared. A subsequent request that has auto index selection enabled via IORING_FILE_INDEX_ALL	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/axboe/linux-block.git/commit/?h=io_uring-6.3&amp;id=761efd55a0227aca3a69deacdaa112fffd44fe37">https://git.kernel.org/pub/scm/linux/kernel/git/axboe/linux-block.git/commit/?h=io_uring-6.3&amp;id=761efd55a0227aca3a69deacdaa112fffd44fe37</a>	O-LIN-LINU-050423/3648

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
			OC can cause a NULL pointer dereference. An unprivileged user can use the flaw to cause a system crash. <b>CVE ID : CVE-2023-1583</b>		
Use After Free	23-Mar-2023	4.7	A use-after-free flaw was found in qdisc_graft in net/sched/sch_api.c in the Linux Kernel due to a race problem. This flaw leads to a denial of service issue. If patch ebda44da44f6 ("net: sched: fix race condition in qdisc_graft()") not applied yet, then kernel could be affected. <b>CVE ID : CVE-2023-0590</b>	<a href="https://lore.kernel.org/all/20221018203258.2793282-1-edumazet@google.com/">https://lore.kernel.org/all/20221018203258.2793282-1-edumazet@google.com/</a>	O-LIN-LINU-050423/3649
Affected Version(s): 6.2					
N/A	22-Mar-2023	7.8	A flaw was found in the Linux kernel, where unauthorized access to the execution of the setuid file with capabilities was found in the Linux kernel's OverlayFS subsystem in how a user copies a capable file from a nosuid mount into another mount. This uid mapping bug allows a local user to escalate their privileges on the system. <b>CVE ID : CVE-2023-0386</b>	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=4f11ada10d0a">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=4f11ada10d0a</a>	O-LIN-LINU-050423/3650
Use After Free	22-Mar-2023	7.8	Use After Free vulnerability in Linux kernel traffic control index filter (tcindex) allows Privilege Escalation. The imperfect	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git</a>	O-LIN-LINU-050423/3651

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
			hash area can be updated while packets are traversing, which will cause a use-after-free when 'tcf_exts_exec()' is called with the destroyed tcf_ext. A local attacker user can use this vulnerability to elevate its privileges to root. This issue affects Linux Kernel: from 4.14 before git commit ee059170b1f7e94e55fa6cadee544e176a6e59c2. <b>CVE ID : CVE-2023-1281</b>	/commit/?id=ee059170b1f7e94e55fa6cadee544e176a6e59c2, <a href="https://kernel.dance/#ee059170b1f7e94e55fa6cadee544e176a6e59c2">https://kernel.dance/#ee059170b1f7e94e55fa6cadee544e176a6e59c2</a>	
NULL Pointer Dereference	24-Mar-2023	5.5	A NULL pointer dereference was found in io_file_bitmap_get in io_uring/filetable.c in the io_uring sub-component in the Linux Kernel. When fixed files are unregistered, some context information (file_alloc_{start,end} and alloc_hint) is not cleared. A subsequent request that has auto index selection enabled via IORING_FILE_INDEX_ALL OC can cause a NULL pointer dereference. An unprivileged user can use the flaw to cause a system crash. <b>CVE ID : CVE-2023-1583</b>	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/axboe/linux-block.git/commit/?h=io_uring-6.3&amp;id=761efd55a0227aca3a69deacdaa112fffd44fe37">https://git.kernel.org/pub/scm/linux/kernel/git/axboe/linux-block.git/commit/?h=io_uring-6.3&amp;id=761efd55a0227aca3a69deacdaa112fffd44fe37</a>	O-LIN-LINU-050423/3652
Affected Version(s): 6.3					
NULL Pointer Dereference	24-Mar-2023	5.5	A NULL pointer dereference was found in io_file_bitmap_get in io_uring/filetable.c in the	<a href="https://git.kernel.org/pub/scm/linux/kernel">https://git.kernel.org/pub/scm/linux/kernel</a>	O-LIN-LINU-050423/3653

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
			<p>io_uring sub-component in the Linux Kernel. When fixed files are unregistered, some context information (file_alloc_{start,end} and alloc_hint) is not cleared. A subsequent request that has auto index selection enabled via IORING_FILE_INDEX_ALL OC can cause a NULL pointer dereference. An unprivileged user can use the flaw to cause a system crash.</p> <p><b>CVE ID : CVE-2023-1583</b></p>	<p>/git/axboe/linux-block.git/commit/?h=io_uring-6.3&amp;id=761efd55a0227aca3a69deacdaa112fffd44fe37</p>	

Affected Version(s): From (including) 4.14 Up to (excluding) 6.2

Use After Free	22-Mar-2023	7.8	<p>Use After Free vulnerability in Linux kernel traffic control index filter (tcindex) allows Privilege Escalation. The imperfect hash area can be updated while packets are traversing, which will cause a use-after-free when 'tcf_exts_exec()' is called with the destroyed tcf_ext. A local attacker user can use this vulnerability to elevate its privileges to root. This issue affects Linux Kernel: from 4.14 before git commit ee059170b1f7e94e55fa6cadee544e176a6e59c2.</p> <p><b>CVE ID : CVE-2023-1281</b></p>	<p><a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ee059170b1f7e94e55fa6cadee544e176a6e59c2">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ee059170b1f7e94e55fa6cadee544e176a6e59c2,</a>  <a href="https://kernel.dance/#ee059170b1f7e94e55fa6cadee544e176a6e59c2">https://kernel.dance/#ee059170b1f7e94e55fa6cadee544e176a6e59c2</a></p>	O-LIN-LINU-050423/3654
----------------	-------------	-----	---	--	------------------------

**Vendor: Microsoft**

**Product: windows**

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): -					
Unquoted Search Path or Element	16-Mar-2023	7.8	VX Search v13.8 and v14.7 was discovered to contain an unquoted service path vulnerability which allows attackers to execute arbitrary commands at elevated privileges via a crafted executable file. <b>CVE ID : CVE-2023-24671</b>	N/A	O-MIC-WIND-050423/3655
Improper Input Validation	22-Mar-2023	7.8	Illustrator version 26.5.2 (and earlier) and 27.2.0 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-25859</b>	<a href="https://helpx.adobe.com/security/products/illustrator/apsb23-19.html">https://helpx.adobe.com/security/products/illustrator/apsb23-19.html</a>	O-MIC-WIND-050423/3656
Integer Overflow or Wraparound	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-25903</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	O-MIC-WIND-050423/3657

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26334</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	O-MIC-WIND-050423/3658
Out-of-bounds Read	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26335</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	O-MIC-WIND-050423/3659
Use After Free	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user.	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	O-MIC-WIND-050423/3660

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
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26336</b>		
Out-of-bounds Write	28-Mar-2023	7.8	Adobe Dimension versions 3.4.7 (and earlier) is affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26337</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	O-MIC-WIND-050423/3661
N/A	16-Mar-2023	7.5	IBM Aspera Faspex 5.0.4 could allow a user to change other user's credentials due to improper access controls. IBM X-Force ID: 249847. <b>CVE ID : CVE-2023-27875</b>	<a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/249847">https://exchange.xforce.ibmcloud.com/vulnerabilities/249847</a> , <a href="https://www.ibm.com/support/pages/node/6963662">https://www.ibm.com/support/pages/node/6963662</a>	O-MIC-WIND-050423/3662
N/A	22-Mar-2023	6.8	A vulnerability in Trend Micro Endpoint Encryption Full Disk Encryption version 6.0.0.3204 and below could allow an attacker with physical access to an affected device to bypass Microsoft Windows? Secure Boot process in an	<a href="https://success.trendmicro.com/solution/000292473">https://success.trendmicro.com/solution/000292473</a>	O-MIC-WIND-050423/3663

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
			<p>attempt to execute other attacks to obtain access to the contents of the device. An attacker must first obtain physical access to the target system in order to exploit this vulnerability. It is also important to note that the contents of the drive(s) encrypted with TMEE FDE would still be protected and would NOT be accessible by the attacker by exploitation of this vulnerability alone.</p> <p><b>CVE ID : CVE-2023-28005</b></p>		
Out-of-bounds Read	28-Mar-2023	5.5	<p>Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.</p> <p><b>CVE ID : CVE-2023-26338</b></p>	<p><a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a></p>	O-MIC-WIND-050423/3664
Out-of-bounds Read	28-Mar-2023	5.5	<p>Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An</p>	<p><a href="https://helpx.adobe.com/security/products/dimension/">https://helpx.adobe.com/security/products/dimension/</a></p>	O-MIC-WIND-050423/3665

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26339</b>	apsb23-20.html	
Out-of-bounds Read	28-Mar-2023	5.5	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. <b>CVE ID : CVE-2023-26340</b>	<a href="https://helpx.adobe.com/security/products/dimension/apsb23-20.html">https://helpx.adobe.com/security/products/dimension/apsb23-20.html</a>	O-MIC-WIND-050423/3666
<b>Vendor: Mikrotik</b>					
<b>Product: routeros</b>					
Affected Version(s): 6.40.5					
Out-of-bounds Write	27-Mar-2023	7.5	An issue in the bridge2 component of MikroTik RouterOS v6.40.5 allows attackers to cause a Denial of Service (DoS) via crafted packets. <b>CVE ID : CVE-2023-24094</b>	N/A	O-MIK-ROUT-050423/3667
<b>Vendor: Omron</b>					
<b>Product: sysmac_cj2h-cpu64-eip_firmware</b>					

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): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3668

**Product: sysmac\_cj2h-cpu64\_firmware**

Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3669

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cj2h-cpu65-eip\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3670
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cj2h-cpu65\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3671
-------------------------	-------------	-----	--	---	------------------------

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cj2h-cpu66-eip\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3672
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cj2h-cpu66\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3673
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cj2h-cpu67-eip\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3674
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cj2h-cpu67\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	O-OMR-SYSM-050423/3675
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cj2h-cpu68-eip\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3676
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cj2h-cpu68\_firmware**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3677

**Product: sysmac\_cj2m-cpu11\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3678
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cj2m-cpu12_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3679
<b>Product: sysmac_cj2m-cpu13_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3680

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cj2m-cpu14\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3681
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cj2m-cpu15\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3682
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cj2m-cpu31\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3683
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cj2m-cpu32\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	O-OMR-SYSM-050423/3684
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cj2m-cpu33\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3685
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cj2m-cpu34\_firmware**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3686

**Product: sysmac\_cj2m-cpu35\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3687
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp1e-e10dr-a_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3688
<b>Product: sysmac_cp1e-e10dr-d_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3689

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1e-e10dt-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3690
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1e-e10dt-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3691
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp1e-e10dt1-a_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3692
<b>Product: sysmac_cp1e-e10dt1-d_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	O-OMR-SYSM-050423/3693

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp1e-e14dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3694
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1e-e14sdr-a\_firmware**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3695

**Product: sysmac\_cp1e-e20dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3696
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp1e-e20sdr-a_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3697
<b>Product: sysmac_cp1e-e30dr-a_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3698

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1e-e30sdr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3699
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1e-e40dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3700
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1e-e40sdr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3701
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1e-e60sdr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	O-OMR-SYSM-050423/3702
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp1e-na20dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3703
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1e-na20dt-d\_firmware**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3704

**Product: sysmac\_cp1e-na20dt1-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3705
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp1h-x40dr-a_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3706
<b>Product: sysmac_cp1h-x40dt-d_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3707

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1h-x40dt1-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3708
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1h-xa40dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3709
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1h-xa40dt-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3710
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1h-xa40dt1-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	O-OMR-SYSM-050423/3711
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp1h-y20dt-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3712
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1l-el20dr-d\_firmware**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3713

**Product: sysmac\_cp1l-em30dr-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3714
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp1l-em30dt-d_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3715
<b>Product: sysmac_cp1l-em30dt1-d_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3716

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1l-em40dr-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3717
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1l-em40dt-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3718
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1l-em40dt1-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3719
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1l-l10dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	O-OMR-SYSM-050423/3720
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp1l-l10dr-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3721
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1l-l10dt-a\_firmware**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3722

**Product: sysmac\_cp1l-l10dt-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3723
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp1l-l10dt1-d_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3724
<b>Product: sysmac_cp1l-l14dr-a_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3725

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1l-l14dr-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3726
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1l-l14dt-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3727
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1l-l14dt-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3728
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1l-l14dt1-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	O-OMR-SYSM-050423/3729
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp11-l20dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3730
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp11-l20dr-d\_firmware**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3731

**Product: sysmac\_cp1l-l20dt-a\_firmware**

Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3732

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp11-l20dt-d_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3733
<b>Product: sysmac_cp11-l20dt1-d_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3734

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp11-m30dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3735
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp11-m30dr-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3736
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp11-m30dt-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3737
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp11-m30dt-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	O-OMR-SYSM-050423/3738
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp1l-m30dt1-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3739
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1l-m40dr-a\_firmware**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3740

**Product: sysmac\_cp1l-m40dr-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3741
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp1l-m40dt-a_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3742
<b>Product: sysmac_cp1l-m40dt-d_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3743

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp1l-m40dt1-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3744
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1l-m60dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3745
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp11-m60dr-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3746
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp11-m60dt-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	O-OMR-SYSM-050423/3747
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp1l-m60dt-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3748
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp1l-m60dt1-d\_firmware**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3749

**Product: sysmac\_cp2e-e14dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3750
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp2e-e20dr-a_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3751
<b>Product: sysmac_cp2e-e30dr-a_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3752

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp2e-e40dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3753
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-e60dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3754
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp2e-n14dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3755
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n14dr-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	O-OMR-SYSM-050423/3756
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp2e-n14dt-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3757
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n14dt-d\_firmware**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3758

**Product: sysmac\_cp2e-n14dt1-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3759
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp2e-n20dr-a_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3760
<b>Product: sysmac_cp2e-n20dr-d_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3761

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp2e-n20dt-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3762
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n20dt-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3763
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp2e-n20dt1-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3764
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n30dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	O-OMR-SYSM-050423/3765
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp2e-n30dr-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3766
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n30dt-a\_firmware**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3767

**Product: sysmac\_cp2e-n30dt-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3768
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp2e-n30dt1-d_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3769
<b>Product: sysmac_cp2e-n40dr-a_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3770

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp2e-n40dr-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3771
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n40dt-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3772
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp2e-n40dt-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3773
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n40dt1-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	O-OMR-SYSM-050423/3774
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp2e-n60dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3775
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-n60dr-d\_firmware**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3776

**Product: sysmac\_cp2e-n60dt-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3777
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp2e-n60dt-d_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3778
<b>Product: sysmac_cp2e-n60dt1-d_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3779

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp2e-s30dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3780
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-s30dt-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3781
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cp2e-s30dt1-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3782
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-s40dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	O-OMR-SYSM-050423/3783
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cp2e-s40dt-d\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3784
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cp2e-s40dt1-d\_firmware**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3785

**Product: sysmac\_cp2e-s60dr-a\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3786
-------------------------	-------------	-----	--	---	------------------------

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Product: sysmac_cp2e-s60dt-d_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3787
<b>Product: sysmac_cp2e-s60dt1-d_firmware</b>					
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a	<a href="https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS-R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3788

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
			non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cs1w-drm21-v1\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3789
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cs1w-eip21\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3790
-------------------------	-------------	-----	--	---	------------------------

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
			specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>		

**Product: sysmac\_cs1w-etn21\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3791
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cs1w-fln22\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the	<a href="https://www.ia.omron.com/produ">https://www.ia.omron.com/produ</a>	O-OMR-SYSM-050423/3792
-------------------------	-------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	ct/vulnerability/OMS R-2023-001_en.pdf	

**Product: sysmac\_cs1w-nc[\]71\_firmware**

Affected Version(s): -

Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMS R-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3793
-------------------------	-------------	-----	---	---	------------------------

**Product: sysmac\_cs1w-spu01-v2\_firmware**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or modifying the user program. <b>CVE ID : CVE-2023-0811</b>	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3794

**Product: sysmac\_cs1w-spu02-v2\_firmware**

Affected Version(s): -					
Improper Access Control	16-Mar-2023	9.1	Omron CJ1M unit v4.0 and prior has improper access controls on the memory region where the UM password is stored. If an adversary issues a PROGRAM AREA WRITE command to a specific memory region, they could overwrite the password. This may lead to disabling UM protections or setting a non-ASCII password (non-keyboard characters) and preventing an engineer from viewing or	<a href="https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf">https://www.ia.omron.com/product/vulnerability/OMSR-2023-001_en.pdf</a>	O-OMR-SYSM-050423/3795

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
			modifying the user program. <b>CVE ID : CVE-2023-0811</b>		
<b>Vendor: paradox</b>					
<b>Product: ipr512_firmware</b>					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	21-Mar-2023	7.5	An issue found in Paradox Security Systems IPR512 allows attackers to cause a denial of service via the login.html and login.xml parameters. <b>CVE ID : CVE-2023-24709</b>	N/A	O-PAR-IPR5-050423/3796
<b>Vendor: Redhat</b>					
<b>Product: enterprise_linux</b>					
Affected Version(s): 8.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/03320.html">https://lists.x.org/archives/xorg-announce/2023-February/03320.html</a>	O-RED-ENTE-050423/3797
Improper Input Validation	23-Mar-2023	5.5	A vulnerability was discovered in ImageMagick where a specially created SVG file	<a href="https://github.com/ImageMagick/ImageMa">https://github.com/ImageMa</a>	O-RED-ENTE-050423/3798

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
			<p>loads itself and causes a segmentation fault. This flaw allows a remote attacker to pass a specially crafted SVG file that leads to a segmentation fault, generating many trash files in "/tmp," resulting in a denial of service. When ImageMagick crashes, it generates a lot of trash files. These trash files can be large if the SVG file contains many render actions. In a denial of service attack, if a remote attacker uploads an SVG file of size t, ImageMagick generates files of size 103*t. If an attacker uploads a 100M SVG, the server will generate about 10G.</p> <p><b>CVE ID : CVE-2023-1289</b></p>	<p>gick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4,  <a href="https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr">https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr</a>,  <a href="https://bugzilla.redhat.com/show_bug.cgi?id=2176858">https://bugzilla.redhat.com/show_bug.cgi?id=2176858</a></p>	
Affected Version(s): 8.1					
Use After Free	27-Mar-2023	7.8	<p>A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote</p>	<p><a href="https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a>,  <a href="https://lists.x.org/archives/xorg-announce/2023-">https://lists.x.org/archives/xorg-announce/2023-</a></p>	O-RED-ENTE-050423/3799

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
			code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	February/03320.html	
Affected Version(s): 9.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/03320.html">https://lists.x.org/archives/xorg-announce/2023-February/03320.html</a>	O-RED-ENTE-050423/3800
Improper Input Validation	23-Mar-2023	5.5	A vulnerability was discovered in ImageMagick where a specially created SVG file loads itself and causes a segmentation fault. This flaw allows a remote attacker to pass a specially crafted SVG file that leads to a segmentation fault, generating many trash files in "/tmp," resulting in a denial of service. When ImageMagick crashes, it generates a lot of trash files. These trash files can be large if the SVG file contains many render actions. In a	<a href="https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4">https://github.com/ImageMagick/ImageMagick/commit/c5b23cbf2119540725e6dc81f4deb25798ead6a4</a> , <a href="https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr">https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-j96m-mjp6-99xr</a> , <a href="https://bug">https://bug</a>	O-RED-ENTE-050423/3801

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
			denial of service attack, if a remote attacker uploads an SVG file of size t, ImageMagick generates files of size 103*t. If an attacker uploads a 100M SVG, the server will generate about 10G. <b>CVE ID : CVE-2023-1289</b>	zilla.redhat.com/show_bug.cgi?id=2176858	
<b>Product: enterprise_linux_aus</b>					
Affected Version(s): 8.4					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/03320.html	O-RED-ENTE-050423/3802
Affected Version(s): 8.6					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can	https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists	O-RED-ENTE-050423/3803

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
			lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	s.x.org/arc-hives/xorg-announce/2023-February/003320.html	

**Product: enterprise\_linux\_desktop**

Affected Version(s): 7.0

Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archive/xorg-announce/2023-February/003320.html	O-RED-ENTE-050423/3804
----------------	-------------	-----	--	---	------------------------

**Product: enterprise\_linux\_eus**

Affected Version(s): 9.0

Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/arc	O-RED-ENTE-050423/3805
----------------	-------------	-----	--	---	------------------------

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
			elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	hives/xorg-announce/2023-February/03320.html	
Affected Version(s): 8.4					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-February/03320.html	O-RED-ENTE-050423/3806
Affected Version(s): 8.6					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote	https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec, https://lists.x.org/archives/xorg-announce/2023-	O-RED-ENTE-050423/3807

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
			code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	February/03320.html	
<b>Product: enterprise_linux_for_ibm_z_systems</b>					
Affected Version(s): 8.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/03320.html">https://lists.x.org/archives/xorg-announce/2023-February/03320.html</a>	O-RED-ENTE-050423/3808
Affected Version(s): 7.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions.	<a href="https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/03320.html">https://lists.x.org/archives/xorg-announce/2023-February/03320.html</a>	O-RED-ENTE-050423/3809

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
			<b>CVE ID : CVE-2023-0494</b>		
<b>Product: enterprise_linux_for_ibm_z_systems_eus</b>					
Affected Version(s): 8.4					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/03320.html">https://lists.x.org/archives/xorg-announce/2023-February/03320.html</a>	O-RED-ENTE-050423/3810
Affected Version(s): 8.6					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/03320.html">https://lists.x.org/archives/xorg-announce/2023-February/03320.html</a>	O-RED-ENTE-050423/3811
<b>Product: enterprise_linux_for_power_big_endian</b>					

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): 7.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/003320.html">https://lists.x.org/archives/xorg-announce/2023-February/003320.html</a>	O-RED-ENTE-050423/3812
<b>Product: enterprise_linux_for_power_little_endian</b>					
Affected Version(s): 8.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/003320.html">https://lists.x.org/archives/xorg-announce/2023-February/003320.html</a>	O-RED-ENTE-050423/3813
Affected Version(s): 9.0					

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
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/003320.html">https://lists.x.org/archives/xorg-announce/2023-February/003320.html</a>	O-RED-ENTE-050423/3814
Affected Version(s): 7.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/003320.html">https://lists.x.org/archives/xorg-announce/2023-February/003320.html</a>	O-RED-ENTE-050423/3815
<b>Product: enterprise_linux_for_power_little_endian_eus</b>					
Affected Version(s): 8.4					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling	<a href="https://gitlab.freedesktop.org/xor">https://gitlab.freedesktop.org/xor</a>	O-RED-ENTE-050423/3816

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
			<p>pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions.</p> <p><b>CVE ID : CVE-2023-0494</b></p>	<p><a href="https://github.com/Xorg/xserver/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">g/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a>,  <a href="https://lists.x.org/archive/xorg-announce/2023-February/003320.html">https://lists.x.org/archive/xorg-announce/2023-February/003320.html</a></p>	
Affected Version(s): 8.6					
Use After Free	27-Mar-2023	7.8	<p>A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions.</p> <p><b>CVE ID : CVE-2023-0494</b></p>	<p><a href="https://github.com/Xorg/xserver/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://github.com/Xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a>,  <a href="https://lists.x.org/archive/xorg-announce/2023-February/003320.html">https://lists.x.org/archive/xorg-announce/2023-February/003320.html</a></p>	O-RED-ENTE-050423/3817
<b>Product: enterprise_linux_for_scientific_computing</b>					
Affected Version(s): 7.0					
Use After Free	27-Mar-2023	7.8	<p>A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by</p>	<p><a href="https://github.com/Xorg/xserver/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://github.com/Xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a></p>	O-RED-ENTE-050423/3818

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
			ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	71131a497 90243cdac 55392ecf7 1ec, <a href="https://lists.x.org/archives/xorg-announce/2023-February/003320.html">https://lists.x.org/archives/xorg-announce/2023-February/003320.html</a>	
<b>Product: enterprise_linux_server</b>					
Affected Version(s): 7.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/003320.html">https://lists.x.org/archives/xorg-announce/2023-February/003320.html</a>	O-RED-ENTE-050423/3819
<b>Product: enterprise_linux_server_au</b>					
Affected Version(s): 8.2					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo()	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a497">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a497</a>	O-RED-ENTE-050423/3820

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	90243cdac55392ecf71ec, <a href="https://lists.x.org/archives/xorg-announce/2023-February/03320.html">https://lists.x.org/archives/xorg-announce/2023-February/03320.html</a>	
<b>Product:</b> <b>enterprise_linux_server_for_power_little_endian_update_services_for_sap_solutions</b>					
Affected Version(s): 8.1					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/03320.html">https://lists.x.org/archives/xorg-announce/2023-February/03320.html</a>	O-RED-ENTE-050423/3821
Affected Version(s): 9.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo()	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf7">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf7</a>	O-RED-ENTE-050423/3822

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	1ec, <a href="https://lists.x.org/archives/xorg-announce/2023-February/003320.html">https://lists.x.org/archives/xorg-announce/2023-February/003320.html</a>	
Affected Version(s): 8.4					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/003320.html">https://lists.x.org/archives/xorg-announce/2023-February/003320.html</a>	O-RED-ENTE-050423/3823
Affected Version(s): 8.6					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/003320.html">https://lists.x.org/archives/xorg-announce/2023-February/003320.html</a>	O-RED-ENTE-050423/3824

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
			where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	announce/2023-February/003320.html	
Affected Version(s): 8.2					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/003320.html">https://lists.x.org/archives/xorg-announce/2023-February/003320.html</a>	O-RED-ENTE-050423/3825
<b>Product: enterprise_linux_server_tus</b>					
Affected Version(s): 8.4					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/003320.html">https://lists.x.org/archives/xorg-announce/2023-February/003320.html</a>	O-RED-ENTE-050423/3826

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
			code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	February/03320.html	
Affected Version(s): 8.6					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/03320.html">https://lists.x.org/archives/xorg-announce/2023-February/03320.html</a>	O-RED-ENTE-050423/3827
Affected Version(s): 8.2					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xorg/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/03320.html">https://lists.x.org/archives/xorg-announce/2023-February/03320.html</a>	O-RED-ENTE-050423/3828

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
<b>Product: enterprise_linux_server_update_services_for_sap_solutions</b>					
Affected Version(s): 8.2					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/003320.html">https://lists.x.org/archives/xorg-announce/2023-February/003320.html</a>	O-RED-ENTE-050423/3829
<b>Product: enterprise_linux_server_workstation</b>					
Affected Version(s): 7.0					
Use After Free	27-Mar-2023	7.8	A vulnerability was found in X.Org. This issue occurs due to a dangling pointer in DeepCopyPointerClasses that can be exploited by ProcXkbSetDeviceInfo() and ProcXkbGetDeviceInfo() to read and write into freed memory. This can lead to local privilege elevation on systems where the X server runs privileged and remote code execution for ssh X forwarding sessions. <b>CVE ID : CVE-2023-0494</b>	<a href="https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec">https://gitlab.freedesktop.org/xserver/-/commit/0ba6d8c37071131a49790243cdac55392ecf71ec</a> , <a href="https://lists.x.org/archives/xorg-announce/2023-February/003320.html">https://lists.x.org/archives/xorg-announce/2023-February/003320.html</a>	O-RED-ENTE-050423/3830
<b>Vendor: Samsung</b>					

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
<b>Product: android</b>					
Affected Version(s): 11.0					
Use After Free	16-Mar-2023	9.8	Use after free vulnerability in decon driver prior to SMR Mar-2023 Release 1 allows attackers to cause memory access fault. <b>CVE ID : CVE-2023-21459</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3831
N/A	16-Mar-2023	8.1	Improper access control vulnerability in Bluetooth prior to SMR Mar-2023 Release 1 allows attackers to send file via Bluetooth without related permission. <b>CVE ID : CVE-2023-21457</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3832
N/A	16-Mar-2023	5.5	Improper access control vulnerability in Call application prior to SMR Mar-2023 Release 1 allows local attackers to access sensitive information without proper permission. <b>CVE ID : CVE-2023-21449</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3833
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Mar-2023	5.5	Path traversal vulnerability in Galaxy Themes Service prior to SMR Mar-2023 Release 1 allows attacker to access arbitrary file with system uid. <b>CVE ID : CVE-2023-21456</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3834
N/A	16-Mar-2023	5.5	Improper authorization vulnerability in AutoPowerOnOffConfirm	<a href="https://security.samsungmobile.com/">https://security.samsungmobile.c</a>	O-SAM-ANDR-050423/3835

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
			Dialog in Settings prior to SMR Mar-2023 Release 1 allows local attacker to turn device off via unprotected activity. <b>CVE ID : CVE-2023-21461</b>	om/securityUpdate.smb?year=2023&month=03	
Improper Authentication	16-Mar-2023	4.4	Improper authentication in SecSettings prior to SMR Mar-2023 Release 1 allows attacker to reset the setting. <b>CVE ID : CVE-2023-21460</b>	https://security.samsungmobile.com/securityUpdate.smb?year=2023&month=03	O-SAM-ANDR-050423/3836
N/A	16-Mar-2023	3.3	Improper usage of implicit intent in Bluetooth prior to SMR Mar-2023 Release 1 allows attacker to get MAC address of connected device. <b>CVE ID : CVE-2023-21452</b>	https://security.samsungmobile.com/securityUpdate.smb?year=2023&month=03	O-SAM-ANDR-050423/3837
Improper Privilege Management	16-Mar-2023	3.3	Improper privilege management vulnerability in PhoneStatusBarPolicy in System UI prior to SMR Mar-2023 Release 1 allows attacker to turn off Do not disturb via unprotected intent. <b>CVE ID : CVE-2023-21458</b>	https://security.samsungmobile.com/securityUpdate.smb?year=2023&month=03	O-SAM-ANDR-050423/3838
N/A	16-Mar-2023	2.4	Improper authorization in Samsung Keyboard prior to SMR Mar-2023 Release 1 allows physical attacker to access users	https://security.samsungmobile.com/securityUpdate.smb?year=20	O-SAM-ANDR-050423/3839

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
			text history on the lockscreen. <b>CVE ID : CVE-2023-21454</b>	23&month=03	
Affected Version(s): 12.0					
Use After Free	16-Mar-2023	9.8	Use after free vulnerability in decon driver prior to SMR Mar-2023 Release 1 allows attackers to cause memory access fault. <b>CVE ID : CVE-2023-21459</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3840
N/A	16-Mar-2023	8.1	Improper access control vulnerability in Bluetooth prior to SMR Mar-2023 Release 1 allows attackers to send file via Bluetooth without related permission. <b>CVE ID : CVE-2023-21457</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3841
N/A	16-Mar-2023	5.5	Improper access control vulnerability in Call application prior to SMR Mar-2023 Release 1 allows local attackers to access sensitive information without proper permission. <b>CVE ID : CVE-2023-21449</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3842
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Mar-2023	5.5	Path traversal vulnerability in Galaxy Themes Service prior to SMR Mar-2023 Release 1 allows attacker to access arbitrary file with system uid.	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3843

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
			<b>CVE ID : CVE-2023-21456</b>		
N/A	16-Mar-2023	5.5	Improper authorization vulnerability in AutoPowerOnOffConfirm Dialog in Settings prior to SMR Mar-2023 Release 1 allows local attacker to turn device off via unprotected activity. <b>CVE ID : CVE-2023-21461</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3844
Improper Authentication	16-Mar-2023	4.4	Improper authentication in SecSettings prior to SMR Mar-2023 Release 1 allows attacker to reset the setting. <b>CVE ID : CVE-2023-21460</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3845
N/A	16-Mar-2023	3.3	Improper usage of implicit intent in Bluetooth prior to SMR Mar-2023 Release 1 allows attacker to get MAC address of connected device. <b>CVE ID : CVE-2023-21452</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3846
Improper Privilege Management	16-Mar-2023	3.3	Improper privilege management vulnerability in PhoneStatusBarPolicy in System UI prior to SMR Mar-2023 Release 1 allows attacker to turn off Do not disturb via unprotected intent. <b>CVE ID : CVE-2023-21458</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3847

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-Mar-2023	2.4	Improper authorization in Samsung Keyboard prior to SMR Mar-2023 Release 1 allows physical attacker to access users text history on the lockscreen. <b>CVE ID : CVE-2023-21454</b>	<a href="https://security.samsungmobile.com/securityUpdate.ssb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.ssb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3848
Affected Version(s): 13.0					
Use After Free	16-Mar-2023	9.8	Use after free vulnerability in decon driver prior to SMR Mar-2023 Release 1 allows attackers to cause memory access fault. <b>CVE ID : CVE-2023-21459</b>	<a href="https://security.samsungmobile.com/securityUpdate.ssb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.ssb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3849
N/A	16-Mar-2023	8.1	Improper access control vulnerability in Bluetooth prior to SMR Mar-2023 Release 1 allows attackers to send file via Bluetooth without related permission. <b>CVE ID : CVE-2023-21457</b>	<a href="https://security.samsungmobile.com/securityUpdate.ssb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.ssb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3850
Improper Input Validation	16-Mar-2023	5.5	Improper input validation vulnerability in SoftSim TA prior to SMR Mar-2023 Release 1 allows local attackers access to protected data. <b>CVE ID : CVE-2023-21453</b>	<a href="https://security.samsungmobile.com/securityUpdate.ssb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.ssb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3851
Improper Limitation of a Pathname to a Restricted	16-Mar-2023	5.5	Path traversal vulnerability in Galaxy Themes Service prior to SMR Mar-2023 Release 1 allows attacker to access	<a href="https://security.samsungmobile.com/securityUpdate.ssb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.ssb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3852

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			arbitrary file with system uid. <b>CVE ID : CVE-2023-21456</b>	23&month=03	
N/A	16-Mar-2023	5.5	Improper authorization vulnerability in AutoPowerOnOffConfirm Dialog in Settings prior to SMR Mar-2023 Release 1 allows local attacker to turn device off via unprotected activity. <b>CVE ID : CVE-2023-21461</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3853
Improper Authentication	16-Mar-2023	4.4	Improper authentication in SecSettings prior to SMR Mar-2023 Release 1 allows attacker to reset the setting. <b>CVE ID : CVE-2023-21460</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3854
N/A	16-Mar-2023	3.3	Improper usage of implicit intent in Bluetooth prior to SMR Mar-2023 Release 1 allows attacker to get MAC address of connected device. <b>CVE ID : CVE-2023-21452</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3855
Improper Privilege Management	16-Mar-2023	3.3	Improper privilege management vulnerability in PhoneStatusBarPolicy in System UI prior to SMR Mar-2023 Release 1 allows attacker to turn off Do not disturb via unprotected intent.	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3856

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
			<b>CVE ID : CVE-2023-21458</b>		
N/A	16-Mar-2023	2.4	Improper authorization in Samsung Keyboard prior to SMR Mar-2023 Release 1 allows physical attacker to access users text history on the lockscreen. <b>CVE ID : CVE-2023-21454</b>	<a href="https://security.samsungmobile.com/securityUpdate.ssb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.ssb?year=2023&amp;month=03</a>	O-SAM-ANDR-050423/3857
<b>Product: exynos_1080_firmware</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fntp attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26496</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	O-SAM-EXYN-050423/3858
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	O-SAM-EXYN-050423/3859

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
			for Video Configuration Attribute. <b>CVE ID : CVE-2023-26497</b>		
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26498</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	O-SAM-EXYN-050423/3860
<b>Product: exynos_980_firmware</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fntp attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26496</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	O-SAM-EXYN-050423/3861

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute. <b>CVE ID : CVE-2023-26497</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	O-SAM-EXYN-050423/3862
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26498</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	O-SAM-EXYN-050423/3863
<b>Product: exynos_auto_t5123_firmware</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	O-SAM-EXYN-050423/3864

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
			corruption can occur due to improper checking of the parameter length while parsing the fmtp attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26496</b>	security-updates/	
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute. <b>CVE ID : CVE-2023-26497</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	O-SAM-EXYN-050423/3865
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26498</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	O-SAM-EXYN-050423/3866

**Product: exynos\_firmware**

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	16-Mar-2023	9.1	Improper authorization implementation in Exynos baseband prior to SMR Mar-2023 Release 1 allows incorrect handling of unencrypted message. <b>CVE ID : CVE-2023-21455</b>	<a href="https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03">https://security.samsungmobile.com/securityUpdate.smb?year=2023&amp;month=03</a>	O-SAM-EXYN-050423/3867
<b>Product: exynos_modem_5123_firmware</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fntp attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26496</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	O-SAM-EXYN-050423/3868
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute.	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	O-SAM-EXYN-050423/3869

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
			<b>CVE ID : CVE-2023-26497</b>		
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26498</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	O-SAM-EXYN-050423/3870
<b>Product: exynos_modem_5300_firmware</b>					
Affected Version(s): -					
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5124. Memory corruption can occur due to improper checking of the parameter length while parsing the fntp attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26496</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	O-SAM-EXYN-050423/3871
Out-of-bounds Write	21-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123,	<a href="https://semiconductor.samsung.com/support">https://semiconductor.samsung.com/support</a>	O-SAM-EXYN-050423/3872

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
			Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T5125. Memory corruption can occur when processing Session Description Negotiation for Video Configuration Attribute. <b>CVE ID : CVE-2023-26497</b>	t/quality-support/product-security-updates/	
Out-of-bounds Write	23-Mar-2023	9.8	An issue was discovered in Samsung Baseband Modem Chipset for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, Exynos Auto T5126. Memory corruption can occur due to improper checking of the number of properties while parsing the chatroom attribute in the SDP (Session Description Protocol) module. <b>CVE ID : CVE-2023-26498</b>	<a href="https://semiconductor.samsung.com/support/quality-support/product-security-updates/">https://semiconductor.samsung.com/support/quality-support/product-security-updates/</a>	O-SAM-EXYN-050423/3873
<b>Vendor: sauter-controls</b>					
<b>Product: ey-as525f001_firmware</b>					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	27-Mar-2023	6.5	An authenticated malicious user could acquire the simple mail transfer protocol (SMTP) Password in cleartext format, despite it being protected and hidden behind asterisks. The attacker could then perform further attacks	N/A	O-SAU-EY-A-050423/3874

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
			using the SMTP credentials. <b>CVE ID : CVE-2023-27927</b>		
Unrestricted Upload of File with Dangerous Type	27-Mar-2023	6.5	An authenticated malicious user could successfully upload a malicious image could lead to a denial-of-service condition. <b>CVE ID : CVE-2023-28652</b>	N/A	O-SAU-EY-A-050423/3875
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	An unauthenticated remote attacker could force all authenticated users, such as administrative users, to perform unauthorized actions by viewing the logs. This action would also grant the attacker privilege escalation. <b>CVE ID : CVE-2023-22300</b>	N/A	O-SAU-EY-A-050423/3876
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Mar-2023	6.1	An unauthenticated remote attacker could provide a malicious link and trick an unsuspecting user into clicking on it. If clicked, the attacker could execute the malicious JavaScript (JS) payload in the target's security context. <b>CVE ID : CVE-2023-28650</b>	N/A	O-SAU-EY-A-050423/3877
Improper Neutralization of Input During	27-Mar-2023	5.4	A malicious user could leverage this vulnerability to escalate privileges or perform unauthorized actions in	N/A	O-SAU-EY-A-050423/3878

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			the context of the targeted privileged users. <b>CVE ID : CVE-2023-28655</b>		
<b>Vendor: silabs</b>					
<b>Product: wireless_smart_ubiquitous_network_linux_border_router_firmware</b>					
Affected Version(s): * Up to (including) 1.5.2					
Missing Authorization	21-Mar-2023	5.3	Missing MAC layer security in Silicon Labs Wi-SUN Linux Border Router v1.5.2 and earlier allows malicious node to route malicious messages through network. <b>CVE ID : CVE-2023-1262</b>	N/A	O-SIL-WIRE-050423/3879
<b>Vendor: Tenda</b>					
<b>Product: ax3_firmware</b>					
Affected Version(s): 16.03.12.11					
Out-of-bounds Write	24-Mar-2023	8.8	Tenda AX3 V16.03.12.11 is vulnerable to Buffer Overflow via /goform/SetFirewallCfg. <b>CVE ID : CVE-2023-27042</b>	N/A	O-TEN-AX3_-050423/3880
<b>Product: g103_firmware</b>					
Affected Version(s): 1.0.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Mar-2023	7.5	Command Injection vulnerability found in Tenda G103 v.1.0.05 allows an attacker to obtain sensitive information via a crafted package <b>CVE ID : CVE-2023-27079</b>	N/A	O-TEN-G103-050423/3881
<b>Product: w20e_firmware</b>					
Affected Version(s): 15.11.0.6					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Mar-2023	9.8	Tenda W20E v15.11.0.6 (US_W20EV4.0br_v15.11.0.6(1068_1546_841)_CN_TDC) is vulnerable to Buffer Overflow via function formIPMacBindModify. <b>CVE ID : CVE-2023-26805</b>	N/A	O-TEN-W20E-050423/3882
Out-of-bounds Write	19-Mar-2023	9.8	Tenda W20E v15.11.0.6(US_W20EV4.0br_v15.11.0.6(1068_1546_841) is vulnerable to Buffer Overflow via function formSetSysTime, <b>CVE ID : CVE-2023-26806</b>	N/A	O-TEN-W20E-050423/3883
<b>Vendor: totolink</b>					
<b>Product: a7100ru_firmware</b>					
Affected Version(s): 7.4cu.2313_b20191024					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Mar-2023	9.8	TOTOLink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the enabled parameter at /setting/setWanIeCfg. <b>CVE ID : CVE-2023-27135</b>	N/A	O-TOT-A710-050423/3884
<b>Vendor: Tp-link</b>					
<b>Product: tl-mr3020_firmware</b>					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in a Command	23-Mar-2023	9.8	A command injection issue was found in TP-Link MR3020 v.1_150921 that allows a remote attacker to execute arbitrary commands via a	N/A	O-TP--TL-M-050423/3885

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			crafted request to the tftp endpoint. <b>CVE ID : CVE-2023-27078</b>		
<b>Vendor: ui</b>					
<b>Product: edgerouter_x_firmware</b>					
Affected Version(s): 2.0.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in Ubiquiti EdgeRouter X 2.0.9-hotfix.6. This issue affects some unknown processing of the component NAT Configuration Handler. The manipulation leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. The identifier VDB-223301 was assigned to this vulnerability. NOTE: The vendor position is that post-authentication issues are not accepted as vulnerabilities. <b>CVE ID : CVE-2023-1456</b>	N/A	O-UI-EDGE-050423/3886
Improper Neutralization of Special Elements used in a Command ('Command Injection')	25-Mar-2023	9.8	<b>** DISPUTED **</b> A vulnerability, which was classified as critical, was found in Ubiquiti EdgeRouter X 2.0.9-hotfix.6. Affected is an unknown function of the component Static Routing	N/A	O-UI-EDGE-050423/3887

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			<p>Configuration Handler. The manipulation of the argument next-hop-interface leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. VDB-223302 is the identifier assigned to this vulnerability. NOTE: The vendor position is that post-authentication issues are not accepted as vulnerabilities.</p> <p><b>CVE ID : CVE-2023-1457</b></p>		